EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Chief, Cyber and Intellectual Property Crimes Section
Assistant United States Attorney
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2400
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)

GOVERNMENT'S REPLY IN SUPPORT OF MOTION TO COMPEL AND OPPOSITION TO APPLE INC.'S MOTION TO VACATE ORDER

DECLARATIONS OF STACEY PERINO, CHRISTOPHER PLUHAR, AND TRACY WILKISON, AND EXHIBITS FILED CONCURRENTLY

Hearing Date:	March 22, 2016
Hearing Time:	1:00 p.m.
Location:	Courtroom of the Hon. Sheri Pym

Applicant United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby files its Reply in Support of the Government's Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate this Court's February 16, 2016 Order Compelling Apple To Assist Agents In Its Search.

This Reply and Opposition is based upon the attached memorandum of points and authorities, the concurrently filed declarations of Federal Bureau of Investigation

("FBI") Technical Director of the Cryptologic and Electronic Analysis Unit Stacey Perino, FBI Supervisory Special Agent Christopher Pluhar, and Assistant United States Attorney Tracy Wilkison, with attached exhibits, the files and records in this case, and such further evidence and argument as this Court may permit.

Dated: March 10, 2016

Respectfully submitted,

EILEEN M. DECKER
United States Attorney

PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division

Tracy Wilk

TRACY L. WILKISON
Assistant United States Attorney

Attorneys for Applicant
UNITED STATES OF AMERICA

TABLE OF CONTENTS

DESCRIPTION PAGE

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

As Apple Inc. concedes in its Opposition, it is fully capable of complying with the Court's Order. By Apple's own reckoning, the corporation—which grosses hundreds of billions of dollars a year—would need to set aside as few as six of its 100,000 employees for perhaps as little as two weeks. This burden, which is not unreasonable, is the direct result of Apple's deliberate marketing decision to engineer its products so that the government cannot search them, even with a warrant. Thus, the lawful warrant in this case—issued by a neutral magistrate upon a finding of probable cause, pursuant to the procedure blessed by the Supreme Court just two years ago in *Riley v. California*, 134 S. Ct. 2473 (2014)—will be frustrated unless Apple complies with the Order. In passing the All Writs Act, Congress gave courts a means of ensuring that their lawful warrants were not thwarted by third parties like Apple.

The Court's Order is modest. It applies to a single iPhone, and it allows Apple to decide the least burdensome means of complying. As Apple well knows, the Order does not compel it to unlock other iPhones or to give the government a universal "master key" or "back door." It is a narrow, targeted order that will produce a narrow, targeted piece of software capable of running on just one iPhone, in the security of Apple's corporate headquarters. That iPhone belongs to the County of San Bernardino, which has consented to its being searched. The phone was used by the now-dead terrorist Syed Rizwan Farook, who also consented to its being searched as part of his employment agreement with the County. In short, the Order invades no one's privacy and raises no Fourth Amendment concerns.

The government and the community need to know what is on the terrorist's phone, and the government needs Apple's assistance to find out. For that reason, the Court properly ordered Apple to disable the warrant-proof barriers it designed. Instead of complying, Apple attacked the All Writs Act as archaic, the Court's Order as leading to a "police state," and the FBI's investigation as shoddy, while extolling itself as the primary guardian of Americans' privacy. (*See* Wilkison Decl. Ex. 1.) Apple's rhetoric is not only false, but also corrosive of the very institutions that are best able to safeguard our liberty and our rights: the courts, the Fourth Amendment, longstanding precedent and venerable laws, and the democratically elected branches of government.

Congress intended the All Writs Act to flexibly meet "new problems" like those devised by Apple. As the Supreme Court held, the Act supplies a basis for a court to order a third-party corporation to assist in gathering evidence. As the Ninth Circuit held, that precedent permits a court to order a corporation to program a computer, even if the corporation objects that doing so will cost it money, divert its technicians, and annoy its customers. That controlling precedent and the All Writs Act—not Apple's technological fiat—should determine whether Farook's iPhone will be searched.

Apple and its *amici* try to alarm this Court with issues of network security, encryption, back doors, and privacy, invoking larger debates before Congress and in the news media. That is a diversion. Apple desperately wants—desperately *needs*—this case not to be "about one isolated iPhone." But there is probable cause to believe there is evidence of a terrorist attack on that phone, and our legal system gives this Court the authority to see that it can be searched pursuant to a lawful warrant. And under the compelling circumstances here, the Court should exercise that authority, even if Apple would rather its products be warrant-proof.

This case—like the three-factor Supreme Court test on which it must be decided—is about specific facts, not broad generalities. Here, Apple deliberately raised technological barriers that now stand between a lawful warrant and an iPhone containing evidence related to the terrorist mass murder of 14 Americans. Apple alone can remove those barriers so that the FBI can search the phone, and it can do so without undue burden. Under those *specific* circumstances, Apple can be compelled to give aid. That is not lawless tyranny. Rather, it is ordered liberty vindicating the rule of law. This Court can, and should, stand by the Order. Apple can, and should, comply with it.

II. ARGUMENT

A. The All Writs Act Is an Integral Part of Our Justice System

In both its Opposition and its public statements, Apple seeks to characterize the All Writs Act ("AWA" or "Act"), codified at 28 U.S.C. § 1651, as an obscure law dredged up by the government to achieve unprecedented power. That premise is false. The Act is a vital part of our legal system that is regularly invoked in a variety of contexts. Congress intended for the Act to be broad and flexible, capable of rising to meet new obstacles to the courts' lawful exercise of jurisdiction. The Act is not a judicial usurpation of congressional power, but rather an example of Congress's reliance upon the courts' sound discretion and close familiarity with specific facts to ensure that justice is done.

The AWA is indeed venerable. It was enacted by the First Congress at "the very beginning of this Nation" as part of the Judiciary Act of 1789. *See Levine v. United States*, 362 U.S. 610, 615 (1960). The Act codified basic judicial powers critical to justice and the legal system, such as the power to issue writs of habeas corpus and mandamus. Like other foundational laws, it was framed not in a hypertechnical way to address the passing needs of 1789, but in broad, enduring terms that bestowed on the courts the "power to issue . . . all . . . writs . . . which may be necessary for the exercise of their respective jurisdictions, and agreeable to principles and usages of law."

The Supreme Court quickly recognized that "[t]o limit the operation of [the Act] *now*, to that which it would have had in the year 1789, would open a door to many and great inconveniencies, which Congress seems to have foreseen, and to have guarded against, by giving ample powers to the Courts, so to mold their process, as to meet whatever changes might take place." *Bank of U.S. v. Halstead*, 23 U.S. (10 Wheat.) 51, 62 (1825) (interpreting the phrase "agreeable to the usages and principles of law" to be a broad grant of power to the federal courts) (emphasis in original).

In the centuries since, the Act has never fallen into disuse or disrepute. Indeed, few laws are more vital. As the Supreme Court has explained:

> [T]he writ must be agreeable to the usages and principles of "law," a term which is unlimited by the common law or the English law. And since "law" is not a static concept, but expands and develops as new problems arise, we do not believe that the forms of [writs] authorized by [the AWA] are only those recognized in this country in 1789, when the original Judiciary Act containing the substance of this section came into existence. In short, we do not read [the AWA] as an ossification of the practice and procedure of more than a century and a half ago. Rather it is a legislatively approved source of procedural instruments designed to achieve "the rational ends of law."

Price v. Johnston, 334 U.S. 266, 282-85 (1948) (discussing the scope of the writ of habeas corpus under the AWA), *overruled on other grounds by McCleskey v. Zant*, 499 U.S. 467 (1991). *Price* further held that because "justice may on occasion require the use of a variation or a modification" of the writ, and because Congress had chosen to provide broad powers in the AWA, "it follows that we should not write in limitations which Congress did not see fit to make." *Id.* Just months after the Supreme Court decided *Price*, Congress responded not by chastening the Court or restricting the AWA, but by "extend[ing]" it: first, courts could now issue not just "necessary" writs but also "appropriate" writs; second, "all" courts, not just certain enumerated ones, would be empowered by the Act. *See* 80 Pub. L. 80-773, ch. 646, 62 Stat. 944 (June 25, 1948); H.R. Rep. No. 308, 80th Cong., 1st Sess., A46 (1947) (noting the "revised section extends the power to issue writs in aid of jurisdiction").

Apple portrays the AWA as dusty and forgotten so that application of the Act here might seem an unprecedented and congressionally unforeseen assumption of judicial power. This mischaracterization of the Act was rejected by the Supreme Court in *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), which held that the AWA is properly used to compel a telecommunications company to supply personnel and equipment to support a government investigation by installing a pen register. The Court's conclusion was expressly based on *Price*'s holding that the AWA must be "fluid" and evolving, *id.* at 173, thus foreclosing Apple's current effort to confine *New York Telephone* to only pen registers.

In deciding *New York Telephone*, the Supreme Court directly confronted and expressly rejected the policy arguments Apple raises now. Like Apple, the telephone company argued: that Congress had not given courts the power to issue such an order in its prior legislation; that the AWA could not be read so broadly; that it was for Congress to decide whether to provide such authority; and that relying on the AWA was a dangerous step down a slippery slope ending in arbitrary police powers. *See In re Order Authorizing the Use of a Pen Register*, 538 F.2d 956, 962-63 (2d Cir. 1976) (reversed); *New York Telephone*, 434 U.S. at 179 (Stevens, J., dissenting). The Court dismissed these arguments in light of *Price*. *See New York Telephone*, 434 U.S. at 173-75 & n.23 (maj. op.). In the forty years since that decision, it has become clear that the Court was correct because those fears have proved unfounded.

The Supreme Court's approach to the AWA does not create an unlimited source of judicial power, as Apple contends. The Act is self-limiting because it can only be invoked in aid of a court's jurisdiction. Here, that jurisdiction rests on a lawful warrant, issued by a neutral magistrate pursuant to Rule 41. And *New York Telephone* provides a further safeguard, not through bright-line rules but rather through three factors courts must consider before exercising their discretion: (1) how far removed a party is from the investigative need; (2) how unreasonable a burden would be placed on that party; and (3) how necessary the party's assistance is to the government. This three-factor analysis respects Congress's mandate that the Act be flexible and adaptable, while eliminating the concern that random citizens will be forcibly deputized.

Technology is constantly advancing, but these advances have never required the AWA to retreat. To the contrary, as the Supreme Court made clear in *Halstead* and *Price*, the Act must grow and develop to keep pace with "whatever changes might take place." Courts used that "common sense" in applying the Act to programming and electronic data in the trap-and-trace context. *See Michigan Bell Tel. Co. v. United States*, 565 F.2d 385, 389 (6th Cir. 1977); *United States v. Illinois Bell Tel. Co.*, 531 F.2d 809, 813 (7th Cir. 1976). And this Court applied the same common sense in issuing the Order. The AWA is a proper source of this Court's authority.

B. Through the All Writs Act, Congress Has Empowered the Court to Decide the Fact-Specific Matter Before It

1. This Case Must Be Decided on Its Facts

The Order applies to a single device and is based on the specific facts before this Court. Those compelling facts justify ordering Apple to remove the barriers to executing a warrant for an iPhone used by a terrorist who carried out a mass murder. Apple demands that the Court should instead address the broad questions whether Apple should be required to unlock *every* iPhone in *every* instance, or whether Apple should be required to give the government the means to do so. Those questions are not before this Court. Indeed, if Apple's compliance with the AWA in a single case were sufficient to require it to comply in all cases, there would be no dispute here: Apple routinely complied with AWA orders in the past. (*See infra* p. 27.) In the same respect, future cases involving other iPhones will be decided on *their* specific facts.

The "case or controversy" before the Court is narrow and specific, as well it should be. "[T]he very strength of our common law" is "its cautious advance and retreat a few steps at a time." Benjamin Cardozo, *The Growth of the Law* 6 (1924). It is precisely the rich facts of a particular case that provide the basis for a court to resolve it, and these same facts ensure that the law's growth is incremental and thoughtful. That is why courts resolve cases and controversies that are "definite and concrete, not hypothetical or abstract." *Railway Mail Assn. v. Corsi*, 326 U.S. 88, 93 (1945).

Only by stripping this case of its "definite and concrete" facts—the very facts that guide the AWA inquiry—and by recasting the case as a "hypothetical or abstract" policy debate can Apple invoke separation of powers and the political-question doctrine. (Opp. 18-19.) Apple urges the Court to focus on broader policy issues, and then proclaims that the Court is forbidden to resolve them. But the actual issue before this Court—whether Apple can be directed under the AWA to provide specific technical assistance—is not a judicially imponderable question forbidden by separation of powers: courts resolve such questions regularly, as in *New York Telephone* and *In re Application of United States for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities* ("*Mountain Bell*"), 616 F.2d 1122, 1126-29 (9th Cir. 1980). Nor must courts flee from cases involving policy and privacy considerations related to searching smartphones. Less than two years ago, the Supreme Court confronted just such issues in *Riley v. California*. The Court, after carefully considering smartphones' technology and their role in society, held that an "appropriate balance" between privacy concerns and investigative needs was struck by the government's obtaining a search warrant. 134 S. Ct. at 2484. The Court added that its "holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search." *Id.* at 2493. Thus, Apple's privacy questions, far from being unanswerable by any court, have already *been* answered by the Supreme Court, and the government complied with *Riley* by obtaining a warrant here.

This case also does not present a "political question," as suggested by Apple. The ongoing debate regarding law enforcement, national security needs, and privacy does not deprive this Court of authority to issue the Order. In fact, Apple's argument is undone by the very authority it cites: *Diamond v. Chakrabarty*, 447 U.S. 303 (1980). (Opp. 19.) Far from refusing to decide a case because of the policy implications before it, the Supreme Court explained that the "grave risks" and "parade of horribles" conjured up by the petitioner and his *amici* needed to be presented to Congress, while the Court would decide the case instead by applying the broad terms Congress used in 1930 Patent Act. *Id.* at 316-18. As *Diamond* shows, the political-question doctrine is a "narrow exception" to the general rule that "the Judiciary has a responsibility to decide cases properly before it." *Zivotofsky ex rel. Zivotofsky v. Clinton*, 132 S. Ct. 1421, 1427 (2012). It applies not in every case raising policy considerations but only in cases that raise nothing *but* policy considerations, cases where there is "a lack of judicially discoverable and manageable standards for resolving" the issue.[1] *Baker v. Carr*, 369 U.S. 186, 217 (1962). Here, as in *Diamond*, the AWA standards already have been "judicially discover[ed]" and have proven "manageable" for decades—indeed, for centuries. The advent of iOS 9 does not alter the authority of the AWA or require this Court to abstain, nor do public and political interest in this case.

2. *Congressional Inaction Does Not Preclude an AWA Order*

As the Supreme Court has made clear, Congress's broad grant of judicial authority under the AWA was designed to avoid the need for more specific, piecemeal legislation. A lack of more specific legislation is thus no barrier to the Order. Apple insists that this Court lost its power under the AWA because the executive branch chose not to propose amendments to CALEA, and because Congress might someday pass other legislation. (Opp. 8-10.) But the Supreme Court has repeatedly made clear "that failed legislative proposals are a particularly dangerous ground on which to rest an interpretation of a prior statute, reasoning that congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction, including the inference that the existing legislation already incorporated the offered change." *United States v. Craft*, 535 U.S. 274, 287 (2002).

Until very recently, there was widespread agreement that the AWA sufficed in this area. As Apple itself has acknowledged, "it seemed that this had been somewhat settled views and settled authority from multiple judges." (Hanna Decl. Ex. DD at 56.) Indeed, Apple has conceded that the recent decision of a Magistrate Judge in the Eastern District of New York "mark[ed] the first time a judge has questioned the authority of the All Writs Act to grant supplemental orders to accompany . . . warrants" to search iPhones.

[1] A case can also be irresoluble in the rare event that "there is a textually demonstrable constitutional commitment of the issue to a coordinate political department." *Zivotofsky*, 132 S. Ct. at 1427. But no such commitment exists here. The issuance of writs is a traditional part of the courts' authority. *See Halstead*, 23 U.S. at 61-62. The AWA exists to further a court's jurisdiction. Congress has indisputably given this Court jurisdiction to issue search warrants through Rule 41(b), and power to issue writs in furtherance of those warrants through the AWA.

(Wilkison Decl. Ex. 16 at 3; *see* Exhibit A to Apple's Notice of Supplemental Authority ("New York Order").) Thus, there is—at a minimum—an "equally tenable inferenc[e]" that "existing legislation already incorporated" the power to order Apple to assist in executing search warrants. *Craft*, 535 U.S. at 287. That inference is all the more powerful because there was never even a "failed legislative proposal" of a "CALEA II" bill (Opp. 9), merely vague discussions about potential legislation that would have placed broader obligations, not at issue here, on some communications service providers.

The Supreme Court has emphasized the prohibition on drawing meaning from congressional silence in the AWA context. In *F.T.C. v. Dean Foods Co.*, 384 U.S. 597, 600 (1966), a circuit court dissolved an FTC restraining order on the ground that, in two different Congresses, "bills sponsored by the said Commission were introduced, which bills if enacted into law would have conferred upon the Commission such authority as it is attempting to exercise in the case now before this court." The Supreme Court reversed, reaffirming two key principles: (1) congressional inaction, past or future, is uninstructive; and (2) because the AWA creates power *absent* congressional legislation, there is no need for Congress to specifically confer it. "Congress neither enacted nor rejected these proposals; it simply did not act on them. Even if it had, the legislation as proposed would have had no affect whatever on the power that Congress granted the courts by the All Writs Act. We cannot infer from the fact that Congress took no action at all . . . an intent to circumscribe traditional judicial remedies." *Id.* at 609. That holding was echoed in *New York Telephone*, which made clear that the AWA empowers a court to act "unless appropriately confined by Congress." 434 U.S. at 172-73.[2]

[2] In a recent and first-of-its-kind ruling, the New York Order—without addressing *Dean Foods*—held that interpreting the AWA to empower courts absent specific congressional authorization would violate separation-of-powers principles by bestowing legislative functions on the courts. (New York Order 21-30.) The government has sought review from the district court overseeing that matter, and the order has no precedential value here. Moreover, its reasoning suffers from fatal flaws. First, this argument was expressly rejected in *Halstead*, 23 U.S. at 61-62 (stating that Congress's check on abusive writs by federal courts is for it to "correct the evil by more specific legislation" rather than having Congress specifically authorize each exercise of the court's authority), and was raised by the dissent in *New York Telephone*, in 434 U.S. at

(footnote cont'd on next page)

In short, the AWA does not require any *additional* legislation to empower the courts. Rather, as *Dean Foods* and *New York Telephone* held, the courts retain the flexible power bestowed by Congress through the AWA unless Congress expressly takes it away. As explained below, Congress has not enacted legislation that specifically confines the courts' power here. Its silence says nothing.

3. CALEA Does Not Forbid the Order

Contrary to Apple's claims (Opp. 16-19), CALEA did not deprive this Court of its power to issue the Order. Congress's intent in passing CALEA was not to weaken existing judicial powers under the AWA, but to "preserve the status quo" regarding the lawful interception of transmissions. *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 455 (D.C. Cir. 2000). The statute does not address the particular issue before this Court.

As explained above, the AWA "is controlling" unless "a statute *specifically* addresses the *particular* issue at hand." *Pennsylvania Bureau of Correction v. U.S. Marshals Serv.*, 474 U.S. 34, 43 (1985) (emphases added). Put otherwise, it is not

179 & n.1 (arguing, for example, that, in light of the limits of Title III, any application of the AWA to pen registers "must await congressional deliberation"), and rejected by the majority, *id.* at 175 n.23 (maj. op.).

Second, the AWA codified the courts' pre-existing, common-law power to issue writs to enforce the courts' jurisdiction. Thus, the idea that judges would continue to determine the scope of these writs would neither surprise nor frighten the Framers. *See also Price*, 334 U.S. at 282-85. That power is not "legislative" in a historical or modern sense. *See Halstead*, 23 U.S. at 61-62 ("It is said, however, that this is the exercise of legislative power, which could not be delegated by Congress to the Courts of justice. But this objection cannot be sustained.").

Third, the New York Order is too narrowly focused on the AWA in the context of evidence gathering. The AWA also codifies, for example, the writs of mandamus and coram nobis. In both of these areas (appellate jurisdiction and post-conviction relief), there is *extensive* congressional legislation setting forth clear limits on the courts' power, defining not only what they may do but also when they may do it. Regarding appellate jurisdiction, Congress has enacted, at a minimum, 28 U.S.C. §§ 1291, 1292, 1295, 2255; 18 U.S.C. §§ 3141-45, 3731, 3742; and 48 U.SC. § 1613a. Nevertheless, pursuant to the AWA, the courts maintain the power to hear any appeal, at any time, provided there is a "clear abuse of discretion" by the district court. *Bankers Life & Casualty Co v. Holland*, 346 U.S. 379 (1953). Similarly, Congress has aggressively legislated in the area of post-conviction relief, first in the Judiciary Act of 1948 and then in the Anti-Terrorism and Effective Death Penalty Act. *See* 28 U.S.C. §§ 2241-55. And yet, pursuant to the AWA, the courts maintain the power to grant relief through the writ of coram nobis. *See Carrington v. United States*, 503 F.3d 888, 890 (9th Cir. 2007), *opinion amended on denial of reh'g*, 530 F.3d 1183 (9th Cir. 2008).

enough for other laws to brush up against similar issues. Rather, Congress must legislate so "intricately" as to leave "no gap to fill." *The Company v. United States*, 349 F.3d 1132, 1145 n.26 (9th Cir. 2003). A rare instance of a court finding such pervasive legislation is *Application of the United States for Relief*, 427 F.2d 639 (9th Cir. 1970), in which the Ninth Circuit held that Title III occupied the field of intercepted wire communications and precluded use of the AWA to compel a telephone company's assistance. But both Congress and the Supreme Court concluded that the Ninth Circuit's decision was wrong. *See New York Telephone*, 434 U.S. at 178 n.25. Moreover, the Supreme Court held that Title III had no effect on the exercise of the AWA in the adjacent area of pen registers, *id.* at 166, rejecting the dissent's arguments to the contrary, *id.* at 179 n.1 (Stevens, J., dissenting).

CALEA, passed in 1994, does not "meticulously," "intricately," or "specifically" address when a court may order a smartphone manufacturer to remove barriers to accessing stored data on a particular smartphone. Rather, it governs what steps telecommunications carriers involved in transmission and switching must take *in advance* of court orders to ensure their systems can isolate information to allow for the real-time interception of network communications. 47 U.S.C. § 1002(a)(1)-(4); *see Am. Council on Educ. v. F.C.C.*, 451 F.3d 226, 227-28 (D.C. Cir. 2006). As the Ninth Circuit has recognized, regulation in a distinct area of law should not "curtail the government's powers in domestic law enforcement" under the AWA. *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc). CALEA thus does not confine the Court's power under the AWA here.

Apple points to a section in CALEA stating that "this subchapter does not authorize any law enforcement agency . . . to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services." (Opp. 16); 47 U.S.C. § 1002(b)(1)(A), (B). Congress's wording here is clear and deliberate. The provision does not destroy any existing authority—or even speak to courts' power at all. Nor does the provision have any effect outside of CALEA itself: it limits only the authority given to "law enforcement agenc[ies]" by "this subchapter." The purpose of the provision is not to impliedly deprive the courts of power under the AWA, but to clarify that the preceding subsection of CALEA, 47 U.S.C. § 1002(a), does not permit law enforcement to dictate the "specific design" of the listed items.

To apply that limitation to the Court's Order would defy both the statutory language and Supreme Court precedent for four reasons: (1) the Order rests not on CALEA, but on the AWA; (2) the Order is an exercise of judicial, not agency authority; (3) the Order does not dictate "any specific design"; and (4) the Order is not directed at an item or service provider listed in § 1002(b)(1)(A), (B).[3] Accordingly, this limitation within CALEA does not restrict the Court's authority under the AWA, let alone dictate the result in this case.

C. The Order Is Proper Under *New York Telephone* and the AWA

This Court had authority to issue the Order pursuant to the AWA, and Apple has demonstrated no discretionary reason to withdraw it. As Apple recognizes, this Court must consider three equitable factors: (1) how "far removed" Apple is "from the underlying controversy"; (2) how "unreasonable [a] burden" the Order would place on Apple; and (3) how "necessary" its assistance is to searching Farook's iPhone.[4] *See New*

[3] With regard to the development and control of iOS, Apple is not a provider of wire or electronic communication services but a software developer and licensor. While Apple may be a provider of electronic communication services in its capacity as provider of FaceTime and iMessage, the Court's order does not bear at all upon the operation of those programs on Farook's iPhone, let alone generally. *See In the Matter of Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs*. 20 F.C.C. Rcd. 14989, at ¶ 21 (2005) (recognizing that an entity could provide multiple kinds of services, and holding that the CALEA analysis must be performed on individual components, not the entity as a whole). Nor is Apple an "equipment manufacturer" as that term is used in CALEA. In CALEA, that term refers to a "manufacturer[] of [] telecommunications transmissions and switching equipment," *see* 47 U.S.C. § 1005—carrier-level equipment, not end-user phones.

[4] The New York Order wrongly posited that there were actually *two* three-part tests: the *New York Telephone* test discussed here, and a statutory one based on the AWA's text. The New York Order cited in support of its statutory test only cases which

(footnote cont'd on next page)

York Telephone, 434 U.S. at 172-75. This test appropriately guides a court's discretion to ensure that the Act does not lead down the slippery slope Apple and *amici* imagine. Here, the factors support the Court's Order.

1. Apple Is Closely Connected to the Underlying Controversy

Apple is not so far removed from the underlying controversy that it should be excused from assisting in the execution of the search warrant. In *New York Telephone*, the phone company was sufficiently close to the controversy because the criminals used its phone lines. *See* 434 U.S. at 174. The Court did not require that the phone company know criminals were using its phone lines, or that it be involved in the crime. *See id.* Here, as a neutral magistrate found, there is probable cause to believe that Farook's iPhone contains evidence related to his crimes. That alone would be sufficient proximity under the AWA and *New York Telephone*, even if Apple did not also own and control the software on Farook's iPhone.

Apple attempts to distinguish itself from *New York Telephone* and companies that have been compelled to provide technical assistance by claiming that (1) it is "unlike a telecommunications monopoly" and (2) it has "merely . . . placed a good into the stream of commerce," as if Apple surrenders control over its iPhones upon selling them. (Opp. 21.) These distinctions fail on both the facts and the law.

To begin with, courts have already issued AWA orders to "manufacturer[s] [such as Apple] to attempt to unlock . . . cellphone[s] so that . . . warrant[s] may be executed." *See, e.g.*, *In re XXX Inc.*, 2014 WL 5510865, at *1-*3 (S.D.N.Y. 2014); *United States v. Blake*, No. 13-CR-80054, ECF No. 207 at 5 (S.D. Fl. July 14, 2014). These orders show there is no bright-line rule that a third party must be a public utility to fall within the

predate *New York Telephone*. (New York Order at 11.) In fact, the *New York Telephone* test was meant as a specific application of the general AWA standards, supplanting any previous statutory tests. The Supreme Court has articulated a similar context-specific three-factor test for the writ of mandamus which supplants any need to create a statutory test. *See Cheney v. U.S. Dist. Court*, 542 U.S. 367, 380-81 (2004). The New York Order's approach disregards not just *New York Telephone*, but also *Halstead*'s interpretation of "usages and principles of law."

Act's reach. So do other cases. *See, e.g.*, *New York Telephone*, 434 U.S. at 174 (collecting examples of individuals compelled via the AWA); *United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (credit card company); *In re Access to Videotapes*, 2003 WL 22053105, at *3 (D. Md. 2003) (landlord); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012) (individual). Regardless, Apple's size, technology, and ubiquity make it akin to the companies in *New York Telephone* and *Mountain Bell*.

Moreover, Apple maintains a continued connection to its phones well beyond their sale, and has deliberately developed its phones so that Apple alone holds the means for courts' search warrants to be carried out. As Apple's business model and its representations to its investors and customers make clear, Apple intentionally and for commercial advantage retains exclusive control over the software that can be used on iPhones, giving it monopoly-like control over the means of distributing software to the phones. As detailed below, Apple does so by: (1) firmly controlling iPhones' operating systems and first-party software; (2) carefully managing and vetting third-party software before authenticating it for use on iPhones; and (3) continually receiving information from devices running its licensed software and its proprietary services, and retaining continued access to data from those devices about how its customers are using them. Having established suzerainty over its users' phones—and control over the precise features of the phones necessary for unlocking them—Apple cannot now pretend to be a bystander, watching this investigation from afar.

First, Apple develops its own operating system, and "is *unique* in that it designs and develops nearly the *entire solution* for its products, including the hardware, operating system, numerous software applications and related services." (Wilkison Decl. Ex. 2 at 8 (Apple 10-K) (emphases added).) Apple's "business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software and services." (*Id.* at 1.) "The tight integration of hardware and software on iOS devices ensures that each component of the system is trusted, and validates the system as a whole." (Hanna Decl. Ex. K at 5 (describing how each step is analyzed and vetted "[f]rom initial boot-up to iOS software updates to third-party apps").)

Second, and pivotally, Apple's devices will not run software that is not electronically "signed" by Apple. (*Id.* at 6 ("only Apple-signed code can be installed on a device"); Hanna Decl. Ex. DD at 64 ("We agree with the government that the system requires Apple authentication.").) Through its exclusive control of its electronic signature, Apple carefully manages and vets both the software updates and all third-party programs ("apps") that can be used on its devices. This keeps Apple close to its phones long after they are sold. As set forth in its licensing agreement, Apple will—if allowed by the user—periodically check with its devices to send signed updates, and will "automatically download and install [them] onto [the] device[s]." (Wilkison Decl. Ex. 3 at ¶ 2(h).) Apple also permits only two kinds of apps to be loaded onto iOS devices through Apple's App Store: those "developed . . . by Apple" and those "developed . . . by a third party developer." (Wilkison Decl. Ex. 4 at 15.) Apple exercises power over both, because they must be signed by Apple. (Hanna Decl. Ex. K at 18; *see also* Perino Decl. Ex. 30 at 1 ("Before your app can integrate app services, be installed on a device, or be submitted to the App Store, it must be signed with a certificate issued by Apple.").)

Third, Apple maintains a connection with its phones after sale by continuing to receive information from the devices and continuing to access data about how its customers are using their phones. Indeed, Apple *requires* its users to consent to Apple's continued use of data: "When you use your device, your phone number and certain unique identifiers for your iOS Device are sent to Apple in order to allow others to reach you by your phone number when using various communication features of the iOS Software, such as iMessage and FaceTime. . . . Other iOS Software features may require information from your iOS Device." (Wilkison Decl. Ex. 3 at ¶ 4.) Apple similarly expects its customers to consent to its continual monitoring of information in order to get and use certain apps and services.[5] Apple's connection to its iPhones is not abstract: at a minimum, Apple was communicating with Farook's iPhone as late as October 2015, when it last backed up some of the phone's data on its iCloud server. (Pluhar Decl. ¶ 8.)

Thus, by its own design, Apple remains close to its iPhones through careful management and constant vigil over what software is on an iPhone and how that software is used. Indeed, Apple is much less "removed from the controversy"—in this case, the government's inability to search Farook's iPhone—than was the *New York Telephone* company because that company did not deliberately place its phone lines to prevent inconspicuous government access. 434 U.S. at 161-62. Here, Apple has deliberately used its control over its software to block law-enforcement requests for access to the contents of its devices, and it has advertised that feature to sell its products. As Apple put it: "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."[6] (Wilkison Decl. Ex. 5 at 2.)

In short, Apple is not some distant, disconnected third party unexpectedly and arbitrarily dragooned into helping solve a problem for which it bears no responsibility. Rather, Apple is intimately close to the barriers on Farook's locked iPhone because Apple specifically designed the iPhone to create those barriers.

[5] (*See, e.g.*, Wilkison Decl. Ex. 4 at 5 (providing that on any device, iOS or not, that uses iTunes Match, Apple "automatically scans the song files and collects other information . . . to identify media in your iTunes library," and "Apple will log information such as the tracks you play, stop or skip, the devices you use, and the time and duration of playback"); *id.* at 22 (same for iCloud Music Library); *id.* at 5-6 (providing Apple's Genius service will "automatically collect information . . . such as your play history and playlists"); *id.* at 16 ("When you opt in to Popular Near Me via enabling Location Services, Apple will . . . automatically collect information related to certain of your App Store Products, such as your time spent with each App Store Product and the number of times each App Store Product is launched.").)

[6] Apple later modified this language: "Apple will not perform iOS data extractions in response to government search warrants." (Hanna Decl. Ex. AA at 2.)

2. *The Burden Placed on Apple Is Not Undue and Unreasonable*

In seeking to avoid compliance with this Court's Order, Apple must show that the burden placed upon it is undue, unreasonable, and noncompensable. *See Mountain Bell*, 616 F.2d at 1122, 1132 ("Appellants did not show that the trace . . . significantly increased the possibility of a malfunction . . . . Nor did appellants prove that the compensation provided for in the Order was in any way inadequate."); *cf. United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991) ("Consequently, a grand jury subpoena issued through normal channels is presumed to be reasonable, and the burden of showing unreasonableness must be on the recipient who seeks to avoid compliance."). Apple has shown none of those things. Neither coding software, nor facing speculative business concerns, nor providing possible future compliance poses an undue burden for Apple.

Apple is one of the richest and most tech-savvy companies in the world, and it is more than able to comply with the AWA order. Indeed, it concedes it can do so with relatively little effort. Even this modest burden is largely a result of Apple's own decision to design and market a nearly warrant-proof phone. In evaluating whether the burden on Apple is undue, this Court can and should recognize the fundamental importance that access to evidence plays in the American system of justice. Given "our historic commitment to the rule of law" and "our view that the twofold aim (of criminal justice) is that guilt shall not escape or innocence suffer," the Supreme Court has recognized that "[t]he need to develop all relevant facts in the adversary system is both fundamental and comprehensive." *United States v. Nixon*, 418 U.S. 683, 708-09 (1974). The Court further explained that "[t]he ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts." *Id.* at 709. Apple's position that it cannot be required to assist with the execution of a warrant for one of its phones flies in the face of these principles and this tradition.

a. Writing Code Is Not a Per Se Undue Burden

Apple's primary argument regarding undue burden appears to be that it should not be required to write any amount of code to assist the government. Apple insists that "no court has ever held that the AWA permits the government to conscript a private company to build software for it." (Opp. 31.) Indeed, Apple proclaims that no company has ever been asked via the Act to write even "some amount of code to gather information." (Opp. 27.) This claim is false. More than 35 years ago, in *Mountain Bell*—a case binding here but unmentioned in the recent New York Order—the Ninth Circuit confronted and rejected exactly that argument. There, as here, appellant made "[a] great deal" of the burden of coding, 616 F.2d at 1126, but the Circuit demurred. It recognized that the AWA order at issue would need to be "accomplished by *programming* a control computer to 'trap' incoming calls to the designated telephone number. Computers that route the incoming calls from the exchange in which they originate[d] from the dialing telephone [were] *programmed*. In this case twelve computers were *programmed*, including those in the Phoenix metropolitan area." *Id.* at 1127 (emphases added). Further, this additional programming caused the phone company's computers to operate much less efficiently. *Id.* Nevertheless, the Circuit held that the lower court "had the *power* to compel [the corporation] to perform" the programming because "[t]he principles announced in *New York Telephone* . . . compel the same result here." *Id.* at 1128-29 (emphasis added).

Like Apple, the corporation protested, arguing "that the technological differences between pen registers" and trap-and-trace programming "serve to distinguish this case." *Id.* at 1129-30. The company also complained that the AWA order made it bear "the entire responsibility for the search." *Id.* at 1129. It further insisted that the requirement to reprogram its computers "(1) resulted in a serious drain upon existing personnel and equipment; and (2) increased the likelihood of system malfunctions while at the same time impairing the company's ability to correct such problems." *Id.* at 1132. It insisted that the order would deprive it of "irreplaceable services provided by key personnel and [cause] the loss of use of various important pieces of equipment." (Wilkison Decl. Ex. 6 at 24-25.) The Circuit was unpersuaded. "[I]t appears to this court to make little difference whether . . . company technicians acting at the behest of federal officials" are required to ensure that "a computer is programmed to detect electronic impulses which, when decoded [by the software], provide a list of telephone numbers." *Id.*[7]

Moreover, *Mountain Bell* was not even the first case to uphold an AWA order compelling computer programming. The Third Circuit did the same in *In Re Application of the United States*, 610 F.2d 1148, 1154 (3d Cir. 1979). There, as here and in *Mountain Bell*, the corporation was ordered to program a computer to help gather data for the government. *Id.* at 1152-53.[8] The corporation, like Apple, complained that "the technical procedures of tracing require that telephone company personnel, not federal officers, fully execute the traces." *Id.* at 1155. And, foreshadowing Apple's arguments, the company also complained that the work it was being asked to undertake "require[d] more extensive and more burdensome involvement on the part of the . . . company" than did the pen registers in *New York Telephone*. *Id.* at 1150. The Circuit rejected these complaints because, among other things, the corporation's refusal to help would otherwise serve "to frustrate the execution of the courts' warrants and to obstruct criminal investigations." *Id.* at 1155. Thus, there is nothing novel or *per se* unduly burdensome about requiring Apple to write code.

[7] Similarly, in the context of a motion to compel Google, Inc. to produce records pursuant to a civil subpoena, a district court held that "creat[ing] new code to format and extract query and URL data from many computer banks, in total requiring up to eight full time days of engineering time" was a burden that could be overcome through compensation. *Gonzalez v. Google*, 234 F.R.D. 674, 683 (N.D. Cal. 2006). Although the undue-burden analysis under Federal Rules of Civil Procedure 26 and 45 differs from the analysis under the AWA, it is instructive that in a civil lawsuit—where importance of evidence gathering is certainly less compelling than in a criminal investigation of a terrorist act—a district court compelled a private company to create code. "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981).

[8] While the tracing programs required little time to input once developed, as likely is the case here, the programs undoubtedly took longer to develop in the first place. *See Application of the United States*, 610 F.2d at 1152.

Contrary to Apple's argument, the Order does not require it to "provide decryption services" to the government. (Opp. 14.) But that would not be novel, either. Indeed, no less an authority than Chief Justice Marshall held that Aaron Burr's clerk could be forced to decipher a coded letter of Burr's, provided that doing so would not incriminate the clerk. *See United States v. Burr*, 25 F. Cas. 38, 39-40 (C.C. Va. 1807). Or, to take a more recent example, the court in *Fricosu*, 841 F. Supp. 2d at 1235, 1237, held that the AWA empowered it to demand the decryption of a laptop, provided that the act of decryption itself would not be used to incriminate the defendant. Here, Apple will not incriminate itself by removing barriers to the lawful search of Farook's iPhone.

To the extent that Apple seeks to analogize its burden to the one in *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283 (9th Cir. 1979), it is mistaken. In *Plum Creek*, the government sought to compel a company that was the target of an investigation to allow its employees to wear a large monitoring device while working in its sawmill. *Id.* at 1285-86. In addition to distracting the workers, these devices could get caught in the mill's equipment, creating an obvious physical danger to the workers. *Id.* at 1289 & n.4. As the district court explained, the company bore "all the safety risks and [would] pay[] the cost of all industrial accidents." *Id.* at 1286. Weighed against the danger to the workers was the weaker interest of reducing the time required for the investigation: far from being necessary, the devices were simply a convenience. *Id.* at 1289 & nn.5, 6. Under those circumstances, the Court would not extend *New York Telephone*.

Simply put, none of the special considerations in *Plum Creek* are present here: the Order does not put Apple's employees in immediate physical peril; Apple is not being required to assist in an investigation into itself; the government has offered to compensate Apple; and—as explained below—Apple's assistance is not a luxury in an OSHA investigation but a necessity in investigating a terrorist attack. *Mountain Bell*, which postdates *Plum Creek* and relates to a much closer factual scenario, provides better guidance. And as in *Mountain Bell*, the burden on Apple is not undue.

b. *Apple's Proffered Estimate of Employee Time Does Not Establish an Undue Burden*

Apple asserts that it would take six to ten employees two to four weeks to develop new code in order to carry out the Court's Order. (Opp. 13; Neuenschwander Decl. ¶¶ 22-25.) Even taking Apple at its word, this is not an undue burden, especially given Apple's vast resources and the government's willingness to find reasonable compromises and provide reasonable reimbursement.

Apple is a Fortune 5 corporation with tremendous power and means: it has more than 100,000 full-time-equivalent employees and had an annual income of over $200 billion dollars in fiscal year 2015—more than the operating budget for California. (*Compare* Wilkison Decl. Ex. 2 at 9, 24, 41 (Apple 10-K), *with* Ex. 7 (FY 2015-16 budget).) Indeed, Apple's revenues exceed the nominal GDPs of two thirds of the world's nations. To build the ordered software, no more than ten employees would be required to work for no more than four weeks, perhaps as little as two weeks. Just as in *Mountain Bell*—where the company complained it would lose "irreplaceable services provided by key personnel" (Wilkison Decl. Ex. 6 at 24-25)—the burden for Apple here is not unreasonable. Moreover, the government has offered to compensate Apple for such costs that this Court determines have been actually incurred and are reasonably necessary for its efforts. *See New York Telephone Co.*, 434 U.S. at 175 (AWA order not unduly burdensome in part because it provided for reimbursement for the company's efforts); *Mountain Bell*, 616 F.2d at 1132 (same).

The government has always been willing to work with Apple to attempt to reduce any burden of providing access to the evidence on Farook's iPhone. *See Mountain Bell*, 616 F.2d at 1124 (noting parties' collaboration to reduce perceived burdens). Before seeking the Order, the government requested voluntary technical assistance from Apple, and provided the details of its proposal. (Supp. Pluhar Decl. ¶ 12.) Apple refused to discuss the proposal's feasibility and instead directed the FBI to methods of access that the FBI had already tried without success. (*Compare* Neuenschwander Decl. ¶¶ 54-61, *with* Supp. Pluhar Decl. ¶ 12.) The government turned to the Court only as a last resort and sought relief on narrow grounds meant to reduce possible burdens on Apple. The Order allows Apple flexibility in how to assist the FBI. (Order ¶ 4.) The government remains willing to seek a modification of the Order, if Apple can propose a less burdensome or more agreeable way for the FBI to access Farook's iPhone.[9] In contrast, Apple makes little effort to explain which parts of the court's order are burdensome, and in what ways. Nor does Apple propose feasible alternatives that it would find less burdensome.[10] Rather, relying on its exclusive knowledge of its software, Apple simply asserts a single, complicated process, without any further elaboration.

In sum, Apple has failed to show that the only concrete burden it can identify—a relatively low amount of technical labor—is undue, unreasonable, and noncompensable.

c. Impinging on Apple's Marketing of Its Products as Search-Warrant-Proof Is Not an Undue Burden

Apple next claims that complying with search warrants will undermine the public's trust in the security of the company's products and services—a reformulation of its concern, raised in the Eastern District of New York, that compliance will tarnish its brand. This is the same argument made by the corporations and rejected by the courts in *New York Telephone* and *Mountain Bell*, 616 F.2d at 1128. Mountain Bell argued that complying with the order would jeopardize its relationship with its customers, and that it

[9] For the reasons discussed above, the FBI cannot itself modify the software on Farook's iPhone without access to the source code and Apple's private electronic signature. The government did not seek to compel Apple to turn those over because it believed such a request would be less palatable to Apple. If Apple would prefer that course, however, that may provide an alternative that requires less labor by Apple programmers. *See In re Under Seal*, 749 F.3d 276, 281-83 (4th Cir. 2014) (affirming contempt sanctions imposed for failure to comply with order requiring the company to assist law enforcement with effecting a pen register on encrypted e-mail content which included producing private SSL encryption key).

[10] For example, Apple suggests that—in complying with the Order—it would have to undertake "substantial" programming to make the software suitable for "consumer interaction." (Neuenschwander Decl. ¶ 19.) But Apple does not explain why Farook's iPhone would need to be ready for "*consumer* interaction" simply to perform forensic data extraction, and does not address the existence of available tools that Apple could use to perform some of the ordered functions. (Perino Decl. ¶¶ 6.b, 25-29.)

could not continue to operate if the public perceived the company as an extension of law enforcement. (Wilkison Decl. Ex. 6 at 32-33.) Those arguments did not persuade those courts then, and they should not persuade this Court now. *Cf. Univ. of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 195-98 (1990) (rejecting university's argument that producing certain information to the government would have a "chilling effect," and declining to recognize a business-interest privilege for withholding the information).

Apple also argues that the Order is unduly burdensome because it is in Apple's "basic interests" to make the data on its phones as secure as possible.[11] (Opp. 23.) The company in *New York Telephone* similarly asserted in its Supreme Court merits briefing that "[p]rotection of this privacy [*i.e.*, "the privacy of communications"] is fundamental to the telephone business." 1977 WL 189311, at *2. It added that its "principal basis" for opposing the order was "the danger of indiscriminate invasions of privacy." *Id.* at *8. The Court rejected those arguments. 434 U.S. at 174. Moreover, programming software is not "offensive to" Apple generally, *New York Telephone*, 434 U.S. at 174, and here Apple's own customer has asked to have the phone unlocked. Nor will programming this particular software compromise the security of any Apple iPhone other than Farook's for reasons explained below. (*See infra* pp. 24-25.)

d. *Apple's Speculation that Third Parties Could Be Harmed in the Future if It Complies With the Order Does Not Establish an Undue Burden on Apple*

Apple speculates that if it submits to a lawful order to assist with a constitutional, warranted search of a consenting customer's phone in America, Apple will have no choice but to help totalitarian regimes suppress dissidents around the globe, and "hackers, criminals, and foreign agents" will have access to the data on millions of

[11] Apple insists that if this Court does not hold that it is a *per se* undue burden to compel a corporation to act against its business interests, a parade of horribles will ensue. (Opp. 26.) As noted above, this line of argument has been repeatedly rejected by the courts. Moreover, the Fourth Amendment, the proximity and necessity factors, and the courts' ultimate discretion provide ample protection against executive overreaching.

iPhones. (Opp. 1-2, 28.) This putative public burden, Apple argues, is a basis to relieve it from the Order. Apple's fears are overblown for reasons both factual and legal.[12]

To begin with, many of the most compelling examples of cybercrime that Apple describes involve not breaches of physical-device security, but rather breaches of network security. That is the "the daily siege" of "hackers, cyber-criminals, and foreign agents" with which the government and victims contend. (Opp. 1.) Nothing in the Court's Order affects Apple's network security. Rather, the features at issue concern only access to a physical device. Thus, for the government even to benefit from the software set forth in the Order, it first had to recover Farook's iPhone itself. (Perino Decl. ¶¶ 6.c, 31-36.) That fact alone eliminates much of Apple's worry.

Next, contrary to Apple's stated fears, there is no reason to think that the code Apple writes in compliance with the Order will ever leave Apple's possession. Nothing in the Order requires Apple to provide that code to the government or to explain to the government how it works. And Apple has shown it is amply capable of protecting code that could compromise its security. For example, Apple currently protects (1) the source code to iOS and other core Apple software and (2) Apple's electronic signature, which as described above allows software to be run on Apple hardware. (Hanna Decl. Ex. DD at 62-64 (code and signature are "the most confidential trade secrets [Apple] has").) *Those* —which the government has *not* requested—are the keys to the kingdom. If Apple can guard them, it can guard this.

[12] Apple speculates that there is no law-enforcement benefit to removing barriers to unlocking an iPhone because criminals and terrorists will encrypt their data in other ways. (Opp. 25.) If this reasoning were correct, there would be no purpose to wire-taps, either. But the reasoning is flawed, for three reasons. *First*, as the wire-tap context illustrates, just because criminals *can* add another layer of security (such as talking in code), they do not always do so. *Second*, even if there are further layers of encryption, the government may be able to pierce that encryption—but only if it can get into the phone in the first place. *Third*, even assuming counterfactually that unlocking iPhones would not be useful in the future due to changes in criminal and terrorist behavior, it is useful *today* for gathering evidence related to the terrorist mass-murder in San Bernardino.

Even if "criminals, terrorists, and hackers" somehow infiltrated Apple and stole the software necessary to unlock Farook's iPhone (Opp. 25), the *only* thing that software could be used to do is unlock Farook's iPhone. (Perino Decl. ¶¶ 6.a, 18-24.) Far from being a master key, the software simply disarms a booby trap affixed to one door: Farook's. The software "will be coded by Apple with a unique identifier of the phone so that the [software] would only load and execute on the SUBJECT DEVICE [*i.e.*, Farook's iPhone]." (Order ¶ 3.) This phone-specific limitation was not dreamed up by the government, but instead employs Apple's well-publicized security paradigm. A "unique ID (ECID)" associated with each physical iPhone is incorporated into the phone's operating system. (Perino Decl. ¶ 20; Hanna Decl. Ex. K at 6.) "Adding the ECID 'personalizes' the authorization for the requesting device." (*Id.*) Apple has designed its phones so that every operating system must pair with the phone's ECID. (Perino Decl. ¶¶ 18-24; Hanna Decl. Ex. K at 6 (describing how the Apple server "adds the ECID" before it "signs" the iOS to be used for the upgrade).) The operating system and ECID must correspond for the operating system to work. The ordered software would rely upon the same limitation.

Apple implies that the code could be modified to run on other phones, but a second Apple security layer prevents that from happening: Apple devices will only run software that is electronically "signed" by Apple. (Hanna Decl. Ex. K at 6 ("only Apple-signed code can be installed on a device").) "Signing" the software described in the Order will not release Apple's signature to the government or anyone else—Apple signs *all* publicly available iOS software, but that does not disclose the signature itself. (Perino Decl. ¶¶ 9, 13-17, 24, 28.) And if the code were modified to run on a phone with a different ECID, it would lack a valid digital signature. Without that signature, the code would not run at all on *any* iOS phone with intact security. (*Id.*) Thus, it is simply not plausible that Apple's complying with the Order would cripple iPhone security.

Similarly misleading is Apple's argument that the Order will force Apple to provide access to data to foreign governments. As a legal matter, the Order does not—

could not—compel Apple to follow or disregard the laws of foreign countries. The pressure of foreign law on Apple flows from its decision to do business in foreign countries, not from the Order. Apple suggests that, as a practical matter, it will cease to resist foreign governments' efforts to obtain information on iPhone users if this Court rules against it. It offers no evidence for this proposition, and the evidence in the public record raises questions whether it is even resisting foreign governments now. For example, according to Apple's own data, China demanded information from Apple regarding over *4,000* iPhones in the first half of 2015, and Apple produced data 74% of the time. (Wilkison Decl. Ex. 8 at 3.) Apple appears to have made special accommodations in China as well: for example, moving Chinese user data to Chinese government servers, and installing a different WiFi protocol for Chinese iPhones. (*See* Wilkison Decl. Ex. 9 (reporting that in August 2014, Apple moved Chinese users' iCloud data onto state-owned servers); Ex. 10 (reporting that Apple produced a modified iPhone for sale in mainland China that used a "WAPI" WiFi standard as required by the Chinese government); Ex. 11 (reporting Apple was the first Western company to have its products use WAPI and "[t]hus, [Apple] is presumably sharing confidential information with the [Chinese] government").) Such accommodations provide Apple with access to a huge, and growing, market. (Wilkison Decl. Ex. 12.) This Court's Order changes neither the carrots nor the sticks that foreign governments can use on Apple. Thus, it does not follow that if America forgoes Apple's assistance in this terrorism investigation, Apple will refuse to comply with the demands of foreign governments. Nor does it follow that if the Court stands by its Order, Apple must yield to foreign demands, made in different circumstances without the safeguards of American law.

Lawful process in America cannot be confined by potential lawless oppression elsewhere merely because a corporation chooses to manufacture and market its products globally, without regard to its host countries' legal regimes. Apple identifies no case holding that such a "burden" is cognizable under the AWA. The concerns Apple raises are unproven, and in any event would not be an unreasonable burden on Apple created by the Order, but an inevitable consequence of Apple's own business decisions.

e. *Cumulative Future Compliance Costs Should Not Be Considered and Are, In Any Event, Compensable*

Next, Apple argues that the Order is unduly burdensome because, if it complies here, it is likely to face other AWA orders in the future. By accumulating its hypothetical future burdens, Apple suggests that because so much criminal evidence is hidden on its warrant-proof iPhones, it should not be compelled to assist in gathering evidence related to the terrorist attack in San Bernardino. (Opp. 26.) Apple is wrong.

To begin with, Apple has identified no precedent for considering possible prospective burdens as a basis for withholding a narrow AWA order now. Neither the Supreme Court in *New York Telephone* nor the Ninth Circuit in *Mountain Bell* considered prospective cumulative costs, even though "it [was] plain, given the Company's policy of refusing to render voluntary assistance in installing pen registers and the Government's determination to continue to utilize them, that the Company will be subjected to similar orders in the future." *New York Telephone*, 434 U.S. at 165 n.6. Instead, those courts looked only at the costs associated with the particular order. *Id.* at 174; *Mountain Bell*, 616 F.2d at 1133. This follows logically from the individualized, fact-intensive nature of the AWA inquiry. Apple's future costs—which can be compensated in future cases—are mere guesswork, especially since, without knowing the facts, there is no way to predict how the courts in hypothetical future cases will weigh the three *New York Telephone* factors.[13]

Moreover, Apple has proven itself more than able to comply with a large volume of law-enforcement requests. Apple has a dedicated team for doing so (Olle Decl. ¶ 2), and it has published guidelines on how legal process will be handled (Wilkison Decl. Ex.

[13] Apple is reportedly already working to re-design the iPhone to preclude compliance with any similar future court orders, which is another reason to question its claimed cumulative costs *and* its assertion that coding is an undue burden for the company. (Wilkison Decl. Ex. 14.)

13). In the first half of 2015 alone, Apple handled 27,000 "device requests"—often covering multiple devices—and provided data approximately 60% of the time. (Wilkison Decl. Ex. 8 at 3-4.) If Apple can provide data from thousands of iPhones and Apple users to China and other countries, it can comply with the AWA in America. (*Id.*) This is not speculation because, in fact, Apple complied for years with American court orders to extract data from passcode-locked iPhones, dedicating infrastructure and personnel in order to do so. (Wilkison Decl. Ex. 14 at 2-3; *id.* Ex. 16 at 3 n.3; Hanna Decl. Ex. DD at 56.) It never objected or sought compensation. (*Compare* Olle Decl. ¶ 13, *with* Hanna Decl. Ex. DD 58 ("[W]e've never required compensation.").) Apple can handle, and has handled, this burden.[14]

In sum, the only concrete, cognizable burdens Apple can identify are reasonable, not undue, and the remaining burdens are speculative and unrecognized by precedent.

3. Apple's Assistance Is Necessary

Without Apple's assistance, the government cannot carry out the search of Farook's iPhone authorized by the search warrant. Apple has ensured that its assistance is necessary by requiring its electronic signature to run any program on the iPhone. Even if the Court ordered Apple to provide the government with Apple's cryptographic keys and source code, Apple itself has implied that the government could not disable the requisite features because it "would have insufficient knowledge of Apple's software and design protocols to be effective." (Neuenschwander Decl. ¶ 23.)

[14] Apple also complains of having "to testify about this back door as a government witnesses at trial." (Opp. 26). "The giving of testimony and the attendance upon court or grand jury in order to testify are public duties which every person within the jurisdiction of the government is bound to perform upon being properly summoned." *Blair v. United States*, 250 U.S. 279, 281 (1919). Moreover, Apple makes no attempt to quantify such costs, instead relying on the implication that the crown jewels of its intellectual property would be released to the world in court. Experience suggests that this is more of a fear than a reality. During the years when Apple followed court orders to extract data from passcode-locked iPhones, the vast majority of affiliated criminal cases were resolved without any need for Apple to testify. (Hanna Decl. Ex. DD 24-25.) Moreover, as Apple conceded, in cases in which testimony from an Apple representative was necessary, no intellectual property was lost. (*Id.* 25.)

Rather than acknowledge this point, Apple instead blames the San Bernardino County Department of Public Health and the FBI. Apple argues that the FBI could have gained access to some of the information via a forced backup to Farook's iCloud account, but since the FBI changed the iCloud password to gain quick access to what was stored in previous backups in the immediate aftermath of the San Bernardino shooting, this path was blocked. (Opp. 11.) That is both untrue and irrelevant.

For several reasons, a forced iCloud backup would not have been successful even if the password had remained unchanged. Farook's iPhone was found powered off. (Supp. Pluhar Decl. ¶ 2.) Subsequent testing has revealed that once powered off, an iPhone will not back itself up to an iCloud account unless and until it has been unlocked at least once by use of the passcode. (Perino Decl. ¶¶ 6.d, 37-39.) Moreover, the evidence on Farook's iCloud account suggests that he had already changed his iCloud password himself on October 22, 2015—shortly after the last backup—and that the auto-backup feature was disabled. (Pluhar Decl. ¶ 8; Supp. Pluhar Decl. ¶ 9.) A forced backup of Farook's iPhone was never going to be successful, and the decision to obtain whatever iCloud evidence was immediately available via the password change was the reasoned decision of experienced FBI agents investigating a deadly terrorist conspiracy.

Moreover, even if—contrary to how Apple built and designed it—Farook's iPhone could have been forced to sync to Apple's iCloud network, that would not be an adequate substitute to unlocking and searching the phone itself. Both the FBI's testing and Apple's security documentation show that entire categories of evidence—including device-level data such as the "keyboard cache" (which records recent keystrokes)—reside only on the iPhone and not on an iCloud backup, and that some of the backup data would still have been encrypted. (Supp. Pluhar Decl. ¶ 10.) But that data remains on the iPhone. Thus, even with a full set of backups, the government still would have needed to search the phone itself in order to leave no stone unturned in this important investigation.

Most importantly, even assuming counterfactually that something could have been recovered through a forced iCloud backup, there have been no backups since October 19, 2015, and Apple concedes there is no way to force a backup now. Thus, the only way to recover *any* subsequent data—whether subject to backup or otherwise—is to unlock Farook's iPhone. And for the FBI to do that, Apple must remove the barriers it put on that phone.

Apple insists that under *New York Telephone*, the government must show "there is no conceivable way" to search Farook's iPhone without Apple's assistance, and contends that the government has not borne this burden. (Opp. 30); 434 U.S. at 174. Apple's quoting of *New York Telephone* lacks context. There, the FBI could install the pen register on its own—just not in an "inconspicuous" location. *Id.* at 161. Moreover, there is no indication that the FBI first enlisted the entire federal government in search of investigative alternatives. *Id.* at 175 ("The FBI . . . was unable to find a location where *it* could install its own pen registers without tipping off the targets of the investigation." (emphasis added)). The broader reasoning of *New York Telephone* further refutes an absolute necessity standard: the Court expressly relied upon the "necessary *or appropriate*" language in the All Writs Act. *Id.* at 172-74. Regardless, even if absolute necessity were required, the undisputed evidence is that the FBI cannot unlock Farook's phone without Apple's assistance. (Wilkison Decl. Ex. 16 at 2-3; Pluhar Decl. ¶ 9.)

* * *

The "definite and concrete" facts of *this* case—as opposed to the "hypothetical or abstract" future scenarios conjured up by Apple, *see Corsi*, 326 U.S. at 93—amply support the Court's Order. Apple deliberately established a security paradigm that keeps Apple intimately connected to its iPhones. This same paradigm makes Apple's assistance necessary for executing the lawful warrant to search Farook's iPhone. Such assistance imposes a burden that is not unreasonable, particularly for a company of Apple's wealth, size, and technical prowess. The Order does no more than require Apple to unknot some of the tangle it has made, so that the court-authorized investigation into Farook's iPhone can proceed.

D. The Order Does Not Implicate, Let Alone Violate, the First and Fifth Amendments

Apple begins its Opposition by insisting that the issues in this case should be left to Congress (Opp. 9), and ends by insisting that the Constitution takes those issues off the table (Opp. 32-34). Not so. The Order is constitutional, notwithstanding Apple's assertion of corporate speech rights and *Lochner*-era substantive due process.[15]

1. Incidentally Requiring a Corporation to Add Functional Source Code to a Commercial Product Does Not Violate the First Amendment

Apple asserts that functional source code in a corporation's commercial product is core protected speech, such that asking it to modify that software on one device—to permit the execution of a lawful warrant—is compelled speech in violation of the First Amendment. This claim "trivializes the freedom protected in *Barnette* and *Wooley*."[16] *See Rumsfeld v. Forum for Acad. & Institutional Rights, Inc.*, 547 U.S. 47, 62 (2006).

Before reaching the specifics of Apple's claim, it is important to start with a threshold observation: the "essential operations" of the American legal system rest upon people sometimes having to say things that they would rather not say—such as when a witness is subpoenaed and sworn to speak the whole truth and nothing but the truth. *West Virginia Bd. of Ed. v. Barnette*, 319 U.S. 624, 645 (1943) (Murphy, J., concurring) (compelled speech doctrine inapplicable to "essential operations of government" such "as in the case of compulsion to give evidence in court"); *see also Murphy v. Waterfront*

[15] The search of a smartphone *does* implicate the Fourth Amendment, *see Riley*, 134 S. Ct. at 2484, but the government has doubly satisfied the Fourth Amendment by obtaining (1) a warrant, *id.*, and (2) the consent of the phone's owner. Moreover, Apple cannot assert any privacy interests of the phone's deceased user, the terrorist Farook. *See Simmons v. United States*, 390 U.S. 377, 389 (1968) ("[R]ights assured by the Fourth Amendment are personal rights, and that they may be enforced by exclusion of evidence only at the instance of one whose own protection was infringed by the search.").

[16] Apple rightly does not attempt to claim standing to assert the First Amendment rights of iPhone users whose phones are not being searched. To the extent *amici* raise such arguments, they are untethered to the issues actually before the Court and, in any event, foreclosed by the Supreme Court's ruling in *Zurcher v. Stanford Daily*, 436 U.S. 547, 563-65 (1978), rejecting a newspaper's claim that a search of its records would chill its speech rights because it would "resort to self-censorship to conceal its possession of information of potential interest to the police."

Comm'n of New York Harbor, 378 U.S. 52, 93-94 (1964) ("Among the necessary and most important of the powers of . . . the Federal Government to assure the effective functioning of government in an ordered society is the broad power to compel residents to testify in court or before grand juries or agencies."), *abrogated on other grounds by United States v. Balsys*, 524 U.S. 666 (1998). This form of "compelled speech" runs throughout both the criminal and civil justice systems, from grand jury and trial subpoenas to interrogatories and depositions. *See, e.g.*, Apple Inc.'s Motion to Compel in *Apple Inc. v. Samsung Electronics*, Docket No. 467 in Case No. 11–cv–1846–LHK, at 11 (N.D. Cal. Dec. 8, 2011) (Apple's seeking court order compelling Samsung to produce source code to facilitate its compelled deposition of witnesses about that source code). If the First Amendment swept as broadly as Apple suggests, there would be no need, for example, for the Fifth Amendment's privilege against self-incrimination.

Apple's claim is particularly weak because it does not involve a person being compelled to speak publicly, but a for-profit corporation being asked to modify commercial software that will be seen only by Apple. There is reason to doubt that functional programming is even entitled to traditional speech protections. *See, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001) (recognizing that source code's "functional capability is not speech within the meaning of the First Amendment"). "[T]hat [programming] occurs at some level through expression does not elevate all such conduct to the highest levels of First Amendment protection. Doing so would turn centuries of our law and legal tradition on its head, eviscerating the carefully crafted balance between free speech and permissible government regulation." *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1128-29 (N.D. Cal. 2002).

To the extent Apple's software includes expressive elements—such as variable names and comments—the Order permits Apple to express whatever it wants, so long as the software functions. *Cf. Karn v. United States Department of State*, 925 F. Supp. 1, 9-10 (D.D.C. 1996) (assuming, without deciding, that source code was speech because it had English comments interspersed). Indeed, the Order's "broad requirements" do "not dictate any specific message," but leave it open to Apple to decide how to develop the code. *See Envtl. Def. Ctr., Inc. v. U.S. E.P.A.*, 344 F.3d 832, 849-51 (9th Cir. 2003). And even assuming, *arguendo*, that the Order compels speech-like programming, there is no audience: Apple's code will be developed in the utmost secrecy and will never be seen outside the corporation. *Cf. Full Value Advisors, LLC v. S.E.C.*, 633 F.3d 1101, 1108-09 (D.C. Cir. 2011) ("constitutional concerns" with compelled public speech are not triggered when government commission "is [the] only audience"); *United States v. Sindel*, 53 F.3d 874, 878 (8th Cir. 1995) (lesser concern where compelled speech lacks "public dissemination"). This stands in stark contrast to the cases cited by Apple, in which software creators were forbidden from publicly sharing what they had written. For all of these reasons, the Order simply does not compel speech.

At most, the Order compels conduct—namely, the removal of barriers from Farook's iPhone—with an incidental effect on "speech" (*i.e.*, programming). That does not amount to a First Amendment violation for the reasons explained by the Supreme Court in *Rumsfeld*, which rejected a First Amendment challenge to the requirement that law schools host and promote military recruitment even if the schools objected to military policy. Like in *Rumsfeld*, "[t]he compelled speech . . . is plainly incidental to the [Order's] regulation of conduct." 547 U.S. at 62. The Order simply requires Apple to remove barriers from Farook's phone. That is conduct, not speech. As the Supreme Court explained, "Congress, for example, can prohibit employers from discriminating in hiring on the basis of race. The fact that this will require an employer to take down a sign reading 'White Applicants Only' hardly means that the law should be analyzed as one regulating the employer's speech rather than conduct." *Id.*

Further, how Apple's software is engineered "is not inherently expressive." *Id.* at 64. Code determining how many retries a user is permitted before the data on an iPhone is permanently lost "lack[s] the expressive quality of a parade, a newsletter, or the editorial page of a newspaper." *Id.* As in *Rumsfeld*, any expressive dimension to Apple's compliance with the Order arises "only because [Apple] accompanied [its] conduct with speech explaining it." *Id.* at 66. Presumably, Apple will respond that if it modifies Farook's iPhone to allow the government access to the phone, it "could be viewed as sending the message that [it] see[s] nothing wrong with [such access], when [it] do[es]." *Id.* at 64-65. But the Supreme Court derided that argument in *Rumsfeld*, explaining that "[n]othing about recruiting suggests that law schools agree with any speech by recruiters, and nothing in the Solomon Amendment restricts what the law schools may say about the military's policies." *Id.* at 65. So too here. And just as in *Rumsfeld*, the public "can appreciate the difference between speech [Apple] sponsors" and code Apple develops "because [it is] legally required to do so." *Id.* It is extremely unlikely that anyone could understand Apple to be expressing a message of hostility to "data security and the privacy of citizens" (Opp. 33), "given both the nature of [Apple's] activity and the factual context and environment in which it was undertaken." *Jacobs v. Clark Cty. Sch. Dist.*, 526 F.3d 419, 438 (9th Cir. 2008).

Even if, despite the above, the Order placed some burden on Apple's ability to market itself as hostile to government searches, that would not establish a First Amendment violation because the Order "promotes a substantial government interest that would [otherwise] be achieved less effectively." *Rumsfeld*, 547 U.S. at 67. There is no question that searching a terrorist's phone—for which a neutral magistrate has found probable cause—is a compelling government interest. *See Branzburg v. Hayes*, 408 U.S. 665, 700 (1972) (recognizing that "the investigation of a crime" and "securing the safety" of citizens are "fundamental" interests for First Amendment purposes). As set forth above, the FBI cannot search Farook's iPhone without Apple's assistance, and Apple has offered no less speech-burdensome manner for providing that assistance.

For all of these reasons, Apple's First Amendment claim must fail.

2. *There Is No Due Process Right Not to Develop Source Code*

Apple lastly asserts that the Order violates its Fifth Amendment right to due process. Apple is currently availing itself of the considerable process our legal system provides, and it is ludicrous to describe the government's actions here as "arbitrary."

(Opp. 34); *see County of Sacramento v. Lewis*, 523 U.S. 833, 846-49 (1998). If Apple is asking for a *Lochner*-style holding that businesses have a substantive due process right against interference with its marketing strategy or against being asked to develop source code, that claim finds no support in any precedent, let alone "in the traditions and conscience of our people," "the concept of ordered liberty," or "this Nation's history." *Washington v. Glucksberg*, 521 U.S. 702, 721 (1997).

III. CONCLUSION

The All Writs Act empowered this Court to issue the Order, just as it empowered a court to order a corporation to engage in computer programming and technical assistance in *Mountain Bell*. As the Supreme Court has repeatedly recognized—and as Congress's repeated reaffirmation and expansion of the Act have confirmed—the Act's flexibility in confronting new problems shows the Framers' foresight and genius, not a blind spot. As the decades since *New York Telephone* have shown, as indeed the centuries since 1789 have proven, courts' exercise of power under the Act does not lead to a headlong tumble down a slippery slope to tyranny. That is because the Act itself—by relying upon the sound discretion of federal judges and by being subordinate to *specific* congressional legislation addressing the *particular* issue—builds in the necessary safeguards. Moreover, the Fourth Amendment, which Apple concedes has been satisfied here, protects against unreasonable privacy invasions.

In short, the limits Apple seeks are already found in the Constitution, the Act, and the three branches of government: congressional legislation, executive restraint, and judicial discretion. The government respectfully submits that *those* authorities should be entrusted to strike the balance between each citizen's right to privacy and all citizens' right to safety and justice. The rule of law does not repose that power in a single corporation, no matter how successful it has been in selling its products.

Accordingly, the government respectfully requests that this Court DENY Apple's motion to vacate this Court's February 16, 2016 Order, and compel Apple to assist the FBI in unlocking Farook's iPhone.

EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Chief, Cyber and Intellectual Property Crimes Section
Assistant United States Attorney
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2400
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE #5KGD203	ED No. CM 16-10 (SP) DECLARATION OF TRACY L. WILKISON IN SUPPORT OF GOVERNMENT'S REPLY IN SUPPORT OF MOTION TO COMPEL AND OPPOSITION TO APPLE INC.'S MOTION TO VACATE ORDER; EXHIBITS 1-16

Hearing Date:	March 22, 2016
Hearing Time:	1:00 p.m.
Location:	Courtroom of the Hon. Sheri Pym

DECLARATION OF TRACY L. WILKISON

I, Tracy L. Wilkison, declare as follows:

1. I am an Assistant United States Attorney in the United States Attorney's Office for the Central District of California. I am one of the attorneys who represent the government in the instant matter.

2. Attached hereto as Exhibit 1 are true and correct copies of the article *Apple's Lawyer: If We Lose, It Will Lead to a 'Police State,'* by David Goldman and Laurie Segall, published on February 26, 2016, available at http://money.cnn.com/2016/02/26/technology/ted-olson-apple/index.html, and printed on March 9, 2016; and the article *Tim Cook: FBI Is Asking Apple to Create 'Software Equivalent of Cancer,'* by Mikey Campbell, published on February 24, 2016, available at http://appleinsider.com/articles/16/02/24/tim-cook-fbi-is-asking-apple-to-create-software-equivalent-of-cancer, and printed on March 9, 2016.

3. Attached hereto as Exhibit 2 is a true and correct copy of *U.S. Sec. and Exch. Comm'n Form 10-K Annual Report for Apple Inc.* (filed on Oct. 28, 2015), available at http://investor.apple.com/secfiling.cfm?filingID=1193125-15-356351&CIK=320193.

4. Attached hereto as Exhibit 3 is a true and correct copy of the English Language portions of the Apple Inc. ("Apple") document *iOS 9.0 Software License Agreement for iPhone, iPad, and iPod Touch*, available at http://images.apple.com/legal/sla/docs/iOS9.pdf, and printed on March 5, 2016.

5. Attached hereto as Exhibit 4 is a true and correct copy of Apple document *Terms and Conditions*, available at http://www.apple.com/legal/internet-services/itunes/us/terms.html, and printed on March 5, 2016.

6. Attached hereto as Exhibit 5 is a true and correct copy of the Internet archive stored version of Apple's statement *Our Commitment To Customer Privacy Doesn't Stop Because Of A Government Information Request* (March 31, 2015),

available at http://web.archive.org/web/20150331005807/http:/www.apple.com/privacy/government-information-requests/, and printed on February 29, 2016.

7. Attached hereto as Exhibit 6 is a true and correct copy of the Brief of Appellant, *United States v. Mountain States Telephone & Telegraph Company*, No. CA 78-2366.

8. Attached hereto as Exhibit 7 is a true and correct copy of document *California Government's Budget 2015-16 Enacted Budget Detail*, available at http://www.ebudget.ca.gov/2015-16/Enacted/agencies.html, and printed on March 4, 2016.

9. Attached hereto as Exhibit 8 is a true and correct copy of Apple document *Report on Government Information Requests (January 1–June 30, 2015)*, available at https://www.apple.com/nz/privacy/docs/government-information-requests-20150914.pdf, and printed on March 5, 2016.

10. Attached hereto as Exhibit 9 is a true and correct copy of the article *Apple Adds State-Controlled China Telecom as Data Center Provider*, by Lorraine Luk, published on August 15, 2014, available at http://blogs.wsj.com/digits/2014/08/15/apple-adds-china-telecom-as-data-center-provider/, and printed on March 5, 2016.

11. Attached hereto as Exhibit 10 is a true and correct copy of the article *Apple Tweaks Wi-Fi in iPhone to Use China Protocol*, by Owen Fletcher, available at http://www.pcworld.com/article/195524/article.html, and printed on March 9, 2016.

12. Attached hereto as Exhibit 11 is a true and correct copy of the report *Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses*, by Hauke Johannes Gierow, Issue 22 China Monitor (published April 22, 2015), available at http://www.merics.org/fileadmin/templates/download/china-monitor/150407_MERICS_China_Monitor_22_en.pdf, and printed on March 9, 2016.

13. Attached hereto as Exhibit 12 is a true and correct copy of the article *While It Defies U.S. Government, Apple Abides By China's Orders—and Reaps Big Rewards*,

by David Pierson, published on February 26, 2016, available at http://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.html, and printed on March 9, 2016.

14. Attached hereto as Exhibit 13 is a true and correct copy of Apple document *Legal Process Guidelines U.S. Law Enforcement*, published September 29, 2105, available at http://www.apple.com/privacy/docs/legal-process-guidelines-us.pdf, and printed on March 5, 2016.

15. Attached hereto as Exhibit 14 is a true and correct copy of Apple statement *Answers To Your Questions About Apple And Security*, available at http://www.apple.com/customer-letter/answers/, and printed on February 28, 2016.

16. Attached hereto as Exhibit 15 is a true and correct copy of the article *Apple Is Said to Be Trying to Make it Harder to Hack iPhones*, by Matt Apuzzo and Katie Benner, version published on February 24, 2016, available at http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html?_r=0, and printed on February 29, 2016.

17. Attached hereto as Exhibit 16 is a true and correct copy of Apple's Response to Court's October 9, 2015 Memorandum and Order, In Re Order Requiring Apple Inc. To Assist In The Execution Of A Search Warrant Issued By This Court, No. 15-MC-1902 (E.D.N.Y. Oct. 19, 2015).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that this declaration is executed in Los Angeles, California, on March 9, 2016.

Tracy Wilk

Tracy L. Wilkison
Assistant United States Attorney

Exhibit 1

Log In

U.S. + Business Markets Tech Media Personal Finance Small Biz Luxury stock tickers

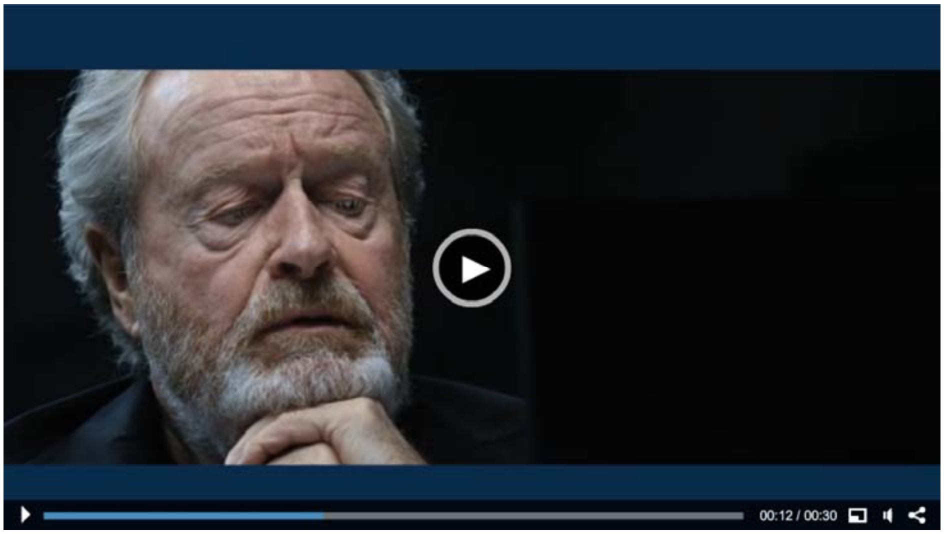
Cyber-Safe

Apple's lawyer: If we lose, it will lead to a 'police state'

by David Goldman and Laurie Segall @CNNTech

February 26, 2016: 12:56 PM ET

Recommend 2.2K



Your video will play in 00:18

Apple's attorney painted a scary picture if Apple loses its fight with the FBI.

In an interview with CNNMoney's Laurie Segall on Friday, Ted Olson warned of a government with "limitless" powers that could "listen to your conversations."

Olson said the demands would mount.

"You can imagine every different law enforcement official telling Apple we want a new product to get into something," Olson said. "Even a state judge could order Apple to build something. There's no stopping point. That would lead to a police state."

The government is trying to force Apple to create new software allowing the FBI to break through the passcode of an iPhone used by the San Bernardino shooter. A magistrate Judge initially ruled in the government's favor, but a final hearing will be held on March 22.

Apple (AAPL, Tech30) says the software will create a back door that will potentially allow anyone to break into millions of iPhones around the world.

"Apple is being asked to put an Achilles heel on the iPhone," Olson said. "The iPhone's security is the reason why many, many people bought the phone."

Ted Olson, Apple's lawyer, says that losing the case will lead to a 'police state.'

Related: Apple tells court that the government can't force it to write code

Olson said that Apple is "very sensitive" to national security and efforts by law enforcement to protect American citizens. He said that Apple has complied with every "legal" request by law enforcement for customers' data.

But in the case against the FBI, Olson said the government overstepped its legal authority. He said Apple's stance hasn't changed -- instead, it's the government's request that has changed and become more expansive than ever.

"It's very easy to say 'terrorism is involved' and therefore you should do whatever the government wants to do," he said. "But just because you're using the word 'terrorism,' you don't want to violate the civil liberties that all of us cherish."

Though he declined to say how far Apple plans to go in its court battle -- "we are a long, long way from that" -- he said that this is the kind of precedent-setting case that could go to the Supreme Court.

If the Supreme Court rules against Apple, though, he said Apple would go along with the ruling.

Meanwhile, Olson noted that Apple continues to upgrade the security of its iPhones. CNNMoney has reported that Apple is working on developing an iPhone that even it can't break into.

"Apple is constantly trying to improve its iPhones ... so that people can't hack in and find out where your children are or what your medical records are," he said. "So if Apple continues to do that, it's just a point at which the government just can't get into your soul. We have got to have a stopping point."

- Erica Fink contributed reporting to this story.

CNNMoney (New York)
First published February 26, 2016: 9:35 AM ET

appleinsider

H +0.09

iPhone 7 | Skylake MacBooks | Apple vs. FBI | iPad Air 3 | Apple Watch 2 | iPhone 6c | Apple Car | iPad Pro

Never miss an update *Follow AppleInsider*

Follow @AppleInsider RSS

Tim Cook: FBI is asking Apple to create 'software equivalent of cancer'

By Mikey Campbell
Wednesday, February 24, 2016, 04 47 pm PT (07 47 pm ET)

In a lengthy interview with ABC News anchor David Muir, Apple CEO Tim Cook reiterated that the repercussions of complying with FBI requests to build an iOS backdoor don't end with one smartphone, but instead have implications that ripple far beyond to hundreds of millions of iOS device owners.

In questioning Cook, Muir first addressed public opinion, which relates the ongoing encryption debate directly — and solely — with 14 people who lost their lives in last year's San Bernardino terrorist attack. Cook, however, remained resolute in his stance that creating a software workaround endangers hundreds of millions of Apple customers.

"It's not like we have information on this phone in the next office over. We have no other information on this phone. None," Cook said. "The only way we know to get additional information is to write a piece of software that is the software equivalent of cancer. That is what is at stake here."

Put more succinctly, Cook said "the future is at stake" in Apple's legal battle for user privacy.

ABC Breaking News | Latest News Videos

When asked about FBI Director James Comey's public statements regarding a one-device workaround, Cook elaborated on the slippery slope argument. If Apple were compelled to build the software requested, it might later be forced to create other intrusive tools like an operating system for surveillance, or code that turns on an iPhone's camera without a user's knowledge, Cook said. These dangers, while intangible at this point, pose a very real threat to the public at large.

"I don't know where this stops, but this should not be happening in this country. This is not what should be happening in America," Cook said, adding that if an encryption law is to be instated, it should first be debated in Congress.

Muir asked why Apple and the FBI were unable to cooperate on the matter earlier, perhaps in a secret lab akin to those used to develop next-generation devices. In response, Cook said that while he can't comment of FBI tactics, the agency chose to take its fight into the public realm. Last week Apple was ordered by a federal magistrate judge to comply with FBI requests for assistance in unlocking an iPhone 5c used by San Bernardino terrorist Syed Rizwan Farook.

Pressed further on the issue, the Apple chief boiled down the debate into one of principle.

"In a perfect world where none of the implications that I'm talking about exist, yes, we would do it — we would obviously do it," Cook said. "But we don't live in a perfect world."

Topics General, Encryption Debate

(62) Comments

Exhibit 2

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

Form 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended September 26, 2015

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from __________ to __________

Commission File Number: **001-36743**

Apple Inc.

(Exact name of Registrant as specified in its charter)

California
(State or other jurisdiction of incorporation or organization)

94-2404110
(I.R.S. Employer Identification No.)

1 Infinite Loop
Cupertino, California
(Address of principal executive offices)

95014
(Zip Code)

(408) 996-1010
(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Common Stock, $0.00001 par value per share	**The NASDAQ Stock Market LLC**
1.000% Notes due 2022	**New York Stock Exchange LLC**
1.625% Notes due 2026	**New York Stock Exchange LLC**
3.05% Notes due 2029	**New York Stock Exchange LLC**
3.60% Notes due 2042	**New York Stock Exchange LLC**
1.375% Notes due 2024	**New York Stock Exchange LLC**
2.000% Notes due 2027	**New York Stock Exchange LLC**
(Title of class)	(Name of exchange on which registered)

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the Registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes ☒ No ☐

Indicate by check mark if the Registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act.

Yes ☐ No ☒

Indicate by check mark whether the Registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the Registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days.

Yes ☒ No ☐

Indicate by check mark whether the Registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the Registrant was required to submit and post such files).

Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of the Registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☒

Indicate by check mark whether the Registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☒	Accelerated filer ☐
Non-accelerated filer ☐ (Do not check if a smaller reporting company)	Smaller reporting company ☐

Indicate by check mark whether the Registrant is a shell company (as defined in Rule 12b-2 of the Act).

Yes ☐ No ☒

The aggregate market value of the voting and non-voting stock held by non-affiliates of the Registrant, as of March 27, 2015, the last business day of the Registrant's most recently completed second fiscal quarter, was approximately $709,923,000,000. Solely for purposes of this disclosure, shares of common stock held by executive officers and directors of the Registrant as of such date have been excluded because such persons may be deemed to be affiliates. This determination of executive officers and directors as affiliates is not necessarily a conclusive determination for any other purposes.

5,575,331,000 shares of common stock were issued and outstanding as of October 9, 2015.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's definitive proxy statement relating to its 2016 annual meeting of shareholders (the "2016 Proxy Statement") are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated. The 2016 Proxy Statement will be filed with the U.S. Securities and Exchange Commission within 120 days after the end of the fiscal year to which this report relates.

Apple Inc.
Form 10-K

For the Fiscal Year Ended September 26, 2015

TABLE OF CONTENTS

Page

Part I

Part II

Part III

Part IV

This Annual Report on Form 10-K ("Form 10-K") contains forward-looking statements, within the meaning of the Private Securities Litigation Reform Act of 1995, that involve risks and uncertainties. Many of the forward-looking statements are located in Part II, Item 7 of this Form 10-K under the heading "Management's Discussion and Analysis of Financial Condition and Results of Operations." Forward-looking statements provide current expectations of future events based on certain assumptions and include any statement that does not directly relate to any historical or current fact. Forward-looking statements can also be identified by words such as "future," "anticipates," "believes," "estimates," "expects," "intends," "will," "would," "could," "can," "may," and similar terms. Forward-looking statements are not guarantees of future performance and the Company's actual results may differ significantly from the results discussed in the forward-looking statements. Factors that might cause such differences include, but are not limited to, those discussed in Part I, Item 1A of this Form 10-K under the heading "Risk Factors," which are incorporated herein by reference. All information presented herein is based on the Company's fiscal calendar. Unless otherwise stated, references to particular years, quarters, months or periods refer to the Company's fiscal years ended in September and the associated quarters, months and periods of those fiscal years. Each of the terms the "Company" and "Apple" as used herein refers collectively to Apple Inc. and its wholly-owned subsidiaries, unless otherwise stated. The Company assumes no obligation to revise or update any forward-looking statements for any reason, except as required by law.

PART I

Item 1. Business

Company Background

The Company designs, manufactures and markets mobile communication and media devices, personal computers and portable digital music players, and sells a variety of related software, services, accessories, networking solutions and third-party digital content and applications. The Company's products and services include iPhone®, iPad®, Mac®, iPod®, Apple Watch®, Apple TV®, a portfolio of consumer and professional software applications, iOS, OS X® and watchOS™ operating systems, iCloud®, Apple Pay® and a variety of accessory, service and support offerings. In September 2015, the Company announced a new Apple TV, tvOS™ operating system and Apple TV App Store®, which are expected to be available by the end of October 2015. The Company sells and delivers digital content and applications through the iTunes Store®, App Store, Mac App Store, iBooks Store™ and Apple Music™ (collectively "Internet Services"). The Company sells its products worldwide through its retail stores, online stores and direct sales force, as well as through third-party cellular network carriers, wholesalers, retailers and value-added resellers. In addition, the Company sells a variety of third-party Apple compatible products, including application software and various accessories through its online and retail stores. The Company sells to consumers, small and mid-sized businesses and education, enterprise and government customers. The Company's fiscal year is the 52 or 53-week period that ends on the last Saturday of September. The Company is a California corporation established in 1977.

Business Strategy

The Company is committed to bringing the best user experience to its customers through its innovative hardware, software and services. The Company's business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software and services to provide its customers products and solutions with innovative design, superior ease-of-use and seamless integration. As part of its strategy, the Company continues to expand its platform for the discovery and delivery of digital content and applications through its Internet Services, which allows customers to discover and download digital content, iOS, Mac and Apple Watch applications, and books through either a Mac or Windows-based computer or through iPhone, iPad and iPod touch® devices ("iOS devices") and Apple Watch. The Company also supports a community for the development of third-party software and hardware products and digital content that complement the Company's offerings. The Company believes a high-quality buying experience with knowledgeable salespersons who can convey the value of the Company's products and services greatly enhances its ability to attract and retain customers. Therefore, the Company's strategy also includes building and expanding its own retail and online stores and its third-party distribution network to effectively reach more customers and provide them with a high-quality sales and post-sales support experience. The Company believes ongoing investment in research and development ("R&D"), marketing and advertising is critical to the development and sale of innovative products and technologies.

Business Organization

The Company manages its business primarily on a geographic basis. In 2015, the Company changed its reportable operating segments as management began reporting business performance and making decisions primarily on a geographic basis, including the results of its retail stores in each respective geographic segment. Accordingly, the Company's reportable operating segments consist of the Americas, Europe, Greater China, Japan and Rest of Asia Pacific. The Americas segment includes both North and South America. The Europe segment includes European countries, as well as India, the Middle East and Africa. The Greater China segment includes China, Hong Kong and Taiwan. The Rest of Asia Pacific segment includes Australia and those Asian countries not included in the Company's other reportable operating segments. Although each reportable operating segment provides similar hardware and software products and similar services, they are managed separately to better align with the location of the Company's customers and distribution partners and the unique market dynamics of each geographic region. Further information regarding the Company's reportable operating segments may be found in Part II, Item 7 of this Form 10-K under the subheading "Segment Operating Performance," and in Part II, Item 8 of this Form 10-K in the Notes to Consolidated Financial Statements in Note 11, "Segment Information and Geographic Data."

Products

iPhone

iPhone is the Company's line of smartphones based on its iOS operating system. iPhone includes Siri®, a voice activated intelligent assistant, and Apple Pay and Touch ID™ on qualifying devices. In September 2015, the Company introduced iPhone 6s and 6s Plus, featuring 3D Touch, which senses force to access features and interact with content and apps. iPhone works with the iTunes Store, App Store and iBooks Store for purchasing, organizing and playing digital content and apps. iPhone is compatible with both Mac and Windows personal computers and Apple's iCloud services, which provide synchronization across users' devices.

iPad

iPad is the Company's line of multi-purpose tablets based on its iOS operating system, which includes iPad Air® and iPad mini™. iPad includes Siri and also includes Touch ID on qualifying devices. In September 2015, the Company announced the new iPad Pro™, featuring a 12.9-inch Retina® display, which is expected to be available in November 2015. iPad works with the iTunes Store, App Store and iBooks Store for purchasing, organizing and playing digital content and apps. iPad is compatible with both Mac and Windows personal computers and Apple's iCloud services.

Mac

Mac is the Company's line of desktop and portable personal computers based on its OS X operating system. The Company's desktop computers include iMac®, 21.5" iMac with Retina 4K Display, 27" iMac with Retina 5K Display, Mac Pro® and Mac mini. The Company's portable computers include MacBook®, MacBook Air®, MacBook Pro® and MacBook Pro with Retina display.

Operating System Software

iOS

iOS is the Company's Multi-Touch™ operating system that serves as the foundation for iOS devices. Devices running iOS are compatible with both Mac and Windows personal computers and Apple's iCloud services. In September 2015, the Company released iOS 9, which provides more search abilities and improved Siri features. iOS 9 also introduced new multitasking features designed specifically for iPad, including Slide Over and Split View, which allow users to work with two apps simultaneously, and Picture-in-Picture that allows users to watch a video while using another application.

OS X

OS X is the Company's Mac operating system and is built on an open-source UNIX-based foundation and provides an intuitive and integrated computer experience. Support for iCloud is built into OS X so users can access content and information from Mac, iOS devices and other supported devices and access downloaded content and apps from the iTunes Store. OS X El Capitan, released in September 2015, is the 12th major release of OS X and incorporates additional window management features, including Split View and the new Spaces Bar in Mission Control®, which provides users an intuitive way to group applications.

watchOS

watchOS is the Company's operating system for Apple Watch. Released in September 2015, watchOS 2 is the first major software update for Apple Watch, providing users with new features, including new watch faces, the ability to add third-party app information on watch faces, Time Travel, and additional communication capabilities in Mail, Friends and Digital Touch. watchOS 2 also gives developers the ability to build native apps for Apple Watch.

tvOS

In September 2015, the Company announced tvOS, its operating system for the new Apple TV, which is expected to be available at the end of October 2015. The tvOS operating system is based on the Company's iOS platform and will enable developers to create new apps and games specifically for Apple TV and deliver them to customers through the new Apple TV App Store.

Application Software

The Company's application software includes iLife®, iWork® and various other software, including Final Cut Pro®, Logic® Pro X and FileMaker® Pro. iLife is the Company's consumer-oriented digital lifestyle software application suite included with all Mac computers and features iMovie®, a digital video editing application, and GarageBand®, a music creation application that allows users to play, record and create music. iWork is the Company's integrated productivity suite included with all Mac computers and is designed to help users create, present and publish documents through Pages®, presentations through Keynote® and spreadsheets through Numbers®. The Company also has Multi-Touch versions of iLife and iWork applications designed specifically for use on iOS devices, which are available as free downloads for all new iPhones and iPads.

Services

Internet Services

The iTunes Store, available for iOS devices, Mac and Windows personal computers and Apple TV, allows customers to purchase and download music and TV shows, rent or purchase movies and download free podcasts. The App Store, available for iOS devices, allows customers to discover and download apps and purchase in-app content. The Mac App Store, available for Mac computers, allows customers to discover, download and install Mac applications. The iBooks Store, available for iOS devices and Mac computers, features e-books from major and independent publishers. Apple Music offers users a curated listening experience with on-demand radio stations that evolve based on a user's play or download activity and a subscription-based internet streaming service that also provides unlimited access to the Apple Music library. In September 2015, the Company announced the Apple TV App Store, which provides customers access to apps and games specifically for the new Apple TV.

iCloud

iCloud is the Company's cloud service which stores music, photos, contacts, calendars, mail, documents and more, keeping them up-to-date and available across multiple iOS devices, Mac and Windows personal computers and Apple TV. iCloud services include iCloud Drive℠, iCloud Photo Library, Family Sharing, Find My iPhone, Find My Friends, Notes, iCloud Keychain® and iCloud Backup for iOS devices.

AppleCare

AppleCare® offers a range of support options for the Company's customers. These include assistance that is built into software products, printed and electronic product manuals, online support including comprehensive product information as well as technical assistance, the AppleCare Protection Plan ("APP") and the AppleCare+ Protection Plan ("AC+"). APP is a fee-based service that typically extends the service coverage of phone support, hardware repairs and dedicated web-based support resources for Mac, Apple TV and display products. AC+ is a fee-based service offering additional coverage under some circumstances for instances of accidental damage in addition to the services offered by APP and is available in certain countries for iPhone, iPad, Apple Watch and iPod.

Apple Pay

Apple Pay is the Company's mobile payment service available in the U.S. and U.K. that offers an easy, secure and private way to pay. Apple Pay allows users to pay for purchases in stores accepting contactless payments and to pay for purchases within participating apps on qualifying devices. Apple Pay accepts credit and debit cards across major card networks and also supports reward programs and store-issued credit and debit cards.

Other Products

Accessories

The Company sells a variety of Apple-branded and third-party Mac-compatible and iOS-compatible accessories, including Apple TV, Apple Watch, headphones, displays, storage devices, Beats products, and various other connectivity and computing products and supplies.

Apple TV

Apple TV connects to consumers' TVs and enables them to access digital content directly for streaming high definition video, playing music and games, and viewing photos. Content from Apple Music and other media services are also available on Apple TV. Apple TV allows streaming digital content from Mac and Windows personal computers through Home Share and through AirPlay® from compatible Mac and iOS devices. In September 2015, the Company announced the new Apple TV running on the Company's tvOS operating system and based on apps built for the television. Additionally, the new Apple TV remote features Siri, allowing users to search and access content with their voice. The new Apple TV is expected to be available at the end of October 2015.

Apple Watch

Apple Watch is a personal electronic device that combines the watchOS user interface and technologies created specifically for a smaller device, including the Digital Crown, a unique navigation tool that allows users to seamlessly scroll, zoom and navigate, and Force Touch, a technology that senses the difference between a tap and a press and allows users to access controls within apps. Apple Watch enables users to communicate in new ways from their wrist, track their health and fitness through activity and workout apps, and includes Siri and Apple Pay.

iPod

iPod is the Company's line of portable digital music and media players, which includes iPod touch, iPod nano® and iPod shuffle®. All iPods work with iTunes to purchase and synchronize content. iPod touch, based on the Company's iOS operating system, is a flash-memory-based iPod that works with the iTunes Store, App Store and iBooks Store for purchasing and playing digital content and apps.

Developer Programs

The Company's developer programs support app developers with building, testing and distributing apps for iOS, Mac, Apple Watch and the new Apple TV. Developer program membership provides access to beta software, the ability to integrate advanced app capabilities (e.g., iCloud, Game Center and Apple Pay), distribution on the App Store, access to App Analytics, and code-level technical support. Developer programs also exist for businesses creating apps for internal use (the Apple Developer Enterprise Program) and developers creating accessories for Apple devices (the MFi Program). All developers, even those who are not developer program members, can sign in with their Apple ID to post on the Apple Developer Forums and use Xcode®, the Company's integrated development environment for creating apps for Apple platforms. Xcode includes project management tools; analysis tools to collect, display and compare app performance data; simulation tools to locally run, test and debug apps; and tools to simplify the design and development of user interfaces. All developers also have access to extensive technical documentation and sample code.

Markets and Distribution

The Company's customers are primarily in the consumer, small and mid-sized business, education, enterprise and government markets. The Company sells its products and resells third-party products in most of its major markets directly to consumers and small and mid-sized businesses through its retail and online stores and its direct sales force. The Company also employs a variety of indirect distribution channels, such as third-party cellular network carriers, wholesalers, retailers and value-added resellers. During 2015, the Company's net sales through its direct and indirect distribution channels accounted for 26% and 74%, respectively, of total net sales.

The Company believes that sales of its innovative and differentiated products are enhanced by knowledgeable salespersons who can convey the value of the hardware and software integration and demonstrate the unique solutions that are available on its products. The Company further believes providing direct contact with its targeted customers is an effective way to demonstrate the advantages of its products over those of its competitors and providing a high-quality sales and after-sales support experience is critical to attracting new and retaining existing customers.

To ensure a high-quality buying experience for its products in which service and education are emphasized, the Company continues to build and improve its distribution capabilities by expanding the number of its own retail stores worldwide. The Company's retail stores are typically located at high-traffic locations in quality shopping malls and urban shopping districts. By operating its own stores and locating them in desirable high-traffic locations the Company is better positioned to ensure a high quality customer buying experience and attract new customers. The stores are designed to simplify and enhance the presentation and marketing of the Company's products and related solutions. The retail stores employ experienced and knowledgeable personnel who provide product advice, service and training and offer a wide selection of third-party hardware, software and other accessories that complement the Company's products.

The Company has also invested in programs to enhance reseller sales by placing high-quality Apple fixtures, merchandising materials and other resources within selected third-party reseller locations. Through the Apple Premium Reseller Program, certain third-party resellers focus on the Apple platform by providing a high level of product expertise, integration and support services.

The Company is committed to delivering solutions to help educators teach and students learn. The Company believes effective integration of technology into classroom instruction can result in higher levels of student achievement and has designed a range of products, services and programs to address the needs of education customers. The Company also supports mobile learning and real-time distribution of, and access to, education related materials through iTunes U, a platform that allows students and teachers to share and distribute educational media online. The Company sells its products to the education market through its direct sales force, select third-party resellers and its online and retail stores.

The Company also sells its hardware and software products to enterprise and government customers in each of its reportable operating segments. The Company's products are deployed in these markets because of their performance, productivity, ease of use and seamless integration into information technology environments. The Company's products are compatible with thousands of third-party business applications and services, and its tools enable the development and secure deployment of custom applications as well as remote device administration.

No single customer accounted for more than 10% of net sales in 2015, 2014 or 2013.

Competition

The markets for the Company's products and services are highly competitive and the Company is confronted by aggressive competition in all areas of its business. These markets are characterized by frequent product introductions and rapid technological advances that have substantially increased the capabilities and use of mobile communication and media devices, personal computers and other digital electronic devices. The Company's competitors that sell mobile devices and personal computers based on other operating systems have aggressively cut prices and lowered their product margins to gain or maintain market share. The Company's financial condition and operating results can be adversely affected by these and other industry-wide downward pressures on gross margins. Principal competitive factors important to the Company include price, product features (including security features), relative price and performance, product quality and reliability, design innovation, a strong third-party software and accessories ecosystem, marketing and distribution capability, service and support and corporate reputation.

The Company is focused on expanding its market opportunities related to personal computers and mobile communication and media devices. These markets are highly competitive and include many large, well-funded and experienced participants. The Company expects competition in these markets to intensify significantly as competitors attempt to imitate some of the features of the Company's products and applications within their own products or, alternatively, collaborate with each other to offer solutions that are more competitive than those they currently offer. These markets are characterized by aggressive pricing practices, frequent product introductions, evolving design approaches and technologies, rapid adoption of technological and product advancements by competitors and price sensitivity on the part of consumers and businesses.

The Company's digital content services have faced significant competition from other companies promoting their own digital music and content products and services, including those offering free peer-to-peer music and video services.

The Company's future financial condition and operating results depend on the Company's ability to continue to develop and offer new innovative products and services in each of the markets in which it competes. The Company believes it offers superior innovation and integration of the entire solution including the hardware (iOS devices, Mac, Apple Watch and Apple TV), software (iOS, OS X, watchOS and tvOS), online services and distribution of digital content and applications (Internet Services). Some of the Company's current and potential competitors have substantial resources and may be able to provide such products and services at little or no profit or even at a loss to compete with the Company's offerings.

Supply of Components

Although most components essential to the Company's business are generally available from multiple sources, a number of components are currently obtained from single or limited sources. In addition, the Company competes for various components with other participants in the markets for mobile communication and media devices and personal computers. Therefore, many components used by the Company, including those that are available from multiple sources, are at times subject to industry-wide shortage and significant pricing fluctuations that could materially adversely affect the Company's financial condition and operating results.

The Company uses some custom components that are not commonly used by its competitors, and the Company often utilizes custom components available from only one source. When a component or product uses new technologies, initial capacity constraints may exist until the suppliers' yields have matured or manufacturing capacity has increased. If the Company's supply of components were delayed or constrained, or if an outsourcing partner delayed shipments of completed products to the Company, the Company's financial condition and operating results could be materially adversely affected. The Company's business and financial performance could also be materially adversely affected depending on the time required to obtain sufficient quantities from the original source, or to identify and obtain sufficient quantities from an alternative source. Continued availability of these components at acceptable prices, or at all, may be affected if those suppliers concentrated on the production of common components instead of components customized to meet the Company's requirements.

The Company has entered into agreements for the supply of many components; however, there can be no guarantee that the Company will be able to extend or renew these agreements on similar terms, or at all. Therefore, the Company remains subject to significant risks of supply shortages and price increases that could materially adversely affect its financial condition and operating results.

While some Mac computers are manufactured in the U.S. and Ireland, substantially all of the Company's hardware products are currently manufactured by outsourcing partners that are located primarily in Asia. A significant concentration of this manufacturing is currently performed by a small number of outsourcing partners, often in single locations. Certain of these outsourcing partners are the sole-sourced suppliers of components and manufacturers for many of the Company's products. Although the Company works closely with its outsourcing partners on manufacturing schedules, the Company's operating results could be adversely affected if its outsourcing partners were unable to meet their production commitments. The Company's purchase commitments typically cover its requirements for periods up to 150 days.

Research and Development

Because the industries in which the Company competes are characterized by rapid technological advances, the Company's ability to compete successfully depends heavily upon its ability to ensure a continual and timely flow of competitive products, services and technologies to the marketplace. The Company continues to develop new technologies to enhance existing products and to expand the range of its product offerings through R&D, licensing of intellectual property and acquisition of third-party businesses and technology. Total R&D expense was $8.1 billion, $6.0 billion and $4.5 billion in 2015, 2014 and 2013, respectively.

Patents, Trademarks, Copyrights and Licenses

The Company currently holds rights to patents and copyrights relating to certain aspects of its hardware devices, accessories, software and services. The Company has registered or has applied for trademarks and service marks in the U.S. and a number of foreign countries. Although the Company believes the ownership of such patents, copyrights, trademarks and service marks is an important factor in its business and that its success does depend in part on such ownership, the Company relies primarily on the innovative skills, technical competence and marketing abilities of its personnel.

The Company regularly files patent applications to protect innovations arising from its research, development and design, and is currently pursuing thousands of patent applications around the world. Over time, the Company has accumulated a large portfolio of issued patents around the world. The Company holds copyrights relating to certain aspects of its products and services. No single patent or copyright is solely responsible for protecting the Company's products. The Company believes the duration of its patents is adequate relative to the expected lives of its products.

Many of the Company's products are designed to include intellectual property obtained from third parties. It may be necessary in the future to seek or renew licenses relating to various aspects of its products, processes and services. While the Company has generally been able to obtain such licenses on commercially reasonable terms in the past, there is no guarantee that such licenses could be obtained in the future on reasonable terms or at all. Because of technological changes in the industries in which the Company competes, current extensive patent coverage and the rapid rate of issuance of new patents, it is possible that certain components of the Company's products, processes and services may unknowingly infringe existing patents or intellectual property rights of others. From time to time, the Company has been notified that it may be infringing certain patents or other intellectual property rights of third parties.

Foreign and Domestic Operations and Geographic Data

During 2015, the Company's domestic and international net sales accounted for 35% and 65%, respectively, of total net sales. Information regarding financial data by geographic segment is set forth in Part II, Item 7 of this Form 10-K under the subheading "Segment Operating Performance," and in Part II, Item 8 of this Form 10-K in the Notes to Consolidated Financial Statements in Note 11, "Segment Information and Geographic Data."

While some Mac computers are manufactured in the U.S. and Ireland, substantially all of the Company's hardware products are currently manufactured by outsourcing partners that are located primarily in Asia. The supply and manufacture of a number of components is performed by sole-sourced outsourcing partners in the U.S., Asia and Europe. Margins on sales of the Company's products in foreign countries and on sales of products that include components obtained from foreign suppliers, can be adversely affected by foreign currency exchange rate fluctuations and by international trade regulations, including tariffs and antidumping penalties. Information regarding concentration in the available sources of supply of materials and products is set forth in Part II, Item 8 of this Form 10-K in the Notes to Consolidated Financial Statements in Note 10, "Commitments and Contingencies."

Business Seasonality and Product Introductions

The Company has historically experienced higher net sales in its first quarter compared to other quarters in its fiscal year due in part to seasonal holiday demand. Additionally, new product introductions can significantly impact net sales, product costs and operating expenses. Product introductions can also impact the Company's net sales to its indirect distribution channels as these channels are filled with new product inventory following a product introduction, and often, channel inventory of a particular product declines as the next related major product launch approaches. Net sales can also be affected when consumers and distributors anticipate a product introduction. However, neither historical seasonal patterns nor historical patterns of product introductions should be considered reliable indicators of the Company's future pattern of product introductions, future net sales or financial performance.

Warranty

The Company offers a limited parts and labor warranty on most of its hardware products. The basic warranty period is typically one year from the date of purchase by the original end-user. The Company also offers a 90-day basic warranty for its service parts used to repair the Company's hardware products. In certain jurisdictions, local law requires that manufacturers guarantee their products for a period prescribed by statute, typically at least two years. In addition, where available, consumers may purchase APP or AC+, which extends service coverage on many of the Company's hardware products.

Backlog

In the Company's experience, the actual amount of product backlog at any particular time is not a meaningful indication of its future business prospects. In particular, backlog often increases immediately following new product introductions as customers anticipate shortages. Backlog is often reduced once customers believe they can obtain sufficient supply. Because of the foregoing, backlog should not be considered a reliable indicator of the Company's ability to achieve any particular level of revenue or financial performance.

Employees

As of September 26, 2015, the Company had approximately 110,000 full-time equivalent employees.

Available Information

The Company's Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to reports filed pursuant to Sections 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), are filed with the Securities and Exchange Commission (the "SEC"). The Company is subject to the informational requirements of the Exchange Act and files or furnishes reports, proxy statements and other information with the SEC. Such reports and other information filed by the Company with the SEC are available free of charge on the Company's website at investor.apple.com/sec.cfm when such reports are available on the SEC's website. The public may read and copy any materials filed by the Company with the SEC at the SEC's Public Reference Room at 100 F Street, NE, Room 1580, Washington, DC 20549. The public may obtain information on the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. The SEC maintains an internet site that contains reports, proxy and information statements and other information regarding issuers that file electronically with the SEC at www.sec.gov. The contents of these websites are not incorporated into this filing. Further, the Company's references to website URLs are intended to be inactive textual references only.

Item 1A. Risk Factors

The following discussion of risk factors contains forward-looking statements. These risk factors may be important to understanding other statements in this Form 10-K. The following information should be read in conjunction with Part II, Item 7, “Management’s Discussion and Analysis of Financial Condition and Results of Operations” and the consolidated financial statements and related notes in Part II, Item 8, “Financial Statements and Supplementary Data” of this Form 10-K.

The business, financial condition and operating results of the Company can be affected by a number of factors, whether currently known or unknown, including but not limited to those described below, any one or more of which could, directly or indirectly, cause the Company’s actual financial condition and operating results to vary materially from past, or from anticipated future, financial condition and operating results. Any of these factors, in whole or in part, could materially and adversely affect the Company’s business, financial condition, operating results and stock price.

Because of the following factors, as well as other factors affecting the Company’s financial condition and operating results, past financial performance should not be considered to be a reliable indicator of future performance, and investors should not use historical trends to anticipate results or trends in future periods.

Global and regional economic conditions could materially adversely affect the Company.

The Company’s operations and performance depend significantly on global and regional economic conditions. Uncertainty about global and regional economic conditions poses a risk as consumers and businesses may postpone spending in response to tighter credit, higher unemployment, financial market volatility, government austerity programs, negative financial news, declines in income or asset values and/or other factors. These worldwide and regional economic conditions could have a material adverse effect on demand for the Company’s products and services. Demand also could differ materially from the Company’s expectations as a result of currency fluctuations because the Company generally raises prices on goods and services sold outside the U.S. to correspond with the effect of a strengthening of the U.S. dollar. Other factors that could influence worldwide or regional demand include changes in fuel and other energy costs, conditions in the real estate and mortgage markets, unemployment, labor and healthcare costs, access to credit, consumer confidence and other macroeconomic factors affecting consumer spending behavior. These and other economic factors could materially adversely affect demand for the Company’s products and services.

In the event of financial turmoil affecting the banking system and financial markets, additional consolidation of the financial services industry, or significant financial service institution failures, there could be tightening in the credit markets, low liquidity and extreme volatility in fixed income, credit, currency and equity markets. This could have a number of effects on the Company’s business, including the insolvency or financial instability of outsourcing partners or suppliers or their inability to obtain credit to finance development and/or manufacture products resulting in product delays; inability of customers, including channel partners, to obtain credit to finance purchases of the Company’s products; failure of derivative counterparties and other financial institutions; and restrictions on the Company’s ability to issue new debt. Other income and expense also could vary materially from expectations depending on gains or losses realized on the sale or exchange of financial instruments; impairment charges resulting from revaluations of debt and equity securities and other investments; changes in interest rates; increases or decreases in cash balances; volatility in foreign exchange rates; and changes in fair value of derivative instruments. Increased volatility in the financial markets and overall economic uncertainty would increase the risk of the actual amounts realized in the future on the Company’s financial instruments differing significantly from the fair values currently assigned to them.

Global markets for the Company’s products and services are highly competitive and subject to rapid technological change, and the Company may be unable to compete effectively in these markets.

The Company’s products and services compete in highly competitive global markets characterized by aggressive price cutting and resulting downward pressure on gross margins, frequent introduction of new products, short product life cycles, evolving industry standards, continual improvement in product price/performance characteristics, rapid adoption of technological and product advancements by competitors and price sensitivity on the part of consumers.

The Company’s ability to compete successfully depends heavily on its ability to ensure a continuing and timely introduction of innovative new products, services and technologies to the marketplace. The Company believes it is unique in that it designs and develops nearly the entire solution for its products, including the hardware, operating system, numerous software applications and related services. As a result, the Company must make significant investments in R&D. The Company currently holds a significant number of patents and copyrights and has registered and/or has applied to register numerous patents, trademarks and service marks. In contrast, many of the Company’s competitors seek to compete primarily through aggressive pricing and very low cost structures, and emulating the Company’s products and infringing on its intellectual property. If the Company is unable to continue to develop and sell innovative new products with attractive margins or if competitors infringe on the Company’s intellectual property, the Company’s ability to maintain a competitive advantage could be adversely affected.

The Company markets certain mobile communication and media devices based on the iOS mobile operating system and also markets related third-party digital content and applications. The Company faces substantial competition in these markets from companies that have significant technical, marketing, distribution and other resources, as well as established hardware, software and digital content supplier relationships; and the Company has a minority market share in the global smartphone market. Additionally, the Company faces significant price competition as competitors reduce their selling prices and attempt to imitate the Company's product features and applications within their own products or, alternatively, collaborate with each other to offer solutions that are more competitive than those they currently offer. The Company competes with business models that include content provided to users for free. The Company also competes with illegitimate ways to obtain third-party digital content and applications. Some of the Company's competitors have greater experience, product breadth and distribution channels than the Company. Because some current and potential competitors have substantial resources and/or experience and a lower cost structure, they may be able to provide products and services at little or no profit or even at a loss. The Company also expects competition to intensify as competitors attempt to imitate the Company's approach to providing components seamlessly within their individual offerings or work collaboratively to offer integrated solutions. The Company's financial condition and operating results depend substantially on the Company's ability to continually improve iOS and iOS devices in order to maintain their functional and design advantages.

The Company is the only authorized maker of hardware using OS X, which has a minority market share in the personal computer market. This market has been contracting and is dominated by computer makers using competing operating systems, most notably Windows. In the market for personal computers and accessories, the Company faces a significant number of competitors, many of which have broader product lines, lower priced products and a larger installed customer base. Historically, consolidation in this market has resulted in larger competitors. Price competition has been particularly intense as competitors selling Windows-based personal computers have aggressively cut prices and lowered product margins. An increasing number of internet-enabled devices that include software applications and are smaller and simpler than traditional personal computers compete for market share with the Company's existing products. The Company's financial condition and operating results also depend on its ability to continually improve the Mac platform to maintain its functional and design advantages.

There can be no assurance the Company will be able to continue to provide products and services that compete effectively.

To remain competitive and stimulate customer demand, the Company must successfully manage frequent product introductions and transitions.

Due to the highly volatile and competitive nature of the industries in which the Company competes, the Company must continually introduce new products, services and technologies, enhance existing products and services, effectively stimulate customer demand for new and upgraded products and successfully manage the transition to these new and upgraded products. The success of new product introductions depends on a number of factors including, but not limited to, timely and successful product development, market acceptance, the Company's ability to manage the risks associated with new product production ramp-up issues, the availability of application software for new products, the effective management of purchase commitments and inventory levels in line with anticipated product demand, the availability of products in appropriate quantities and at expected costs to meet anticipated demand and the risk that new products may have quality or other defects or deficiencies in the early stages of introduction. Accordingly, the Company cannot determine in advance the ultimate effect of new product introductions and transitions.

The Company depends on the performance of distributors, carriers and other resellers.

The Company distributes its products through cellular network carriers, wholesalers, national and regional retailers and value-added resellers, many of whom distribute products from competing manufacturers. The Company also sells its products and third-party products in most of its major markets directly to education, enterprise and government customers and consumers and small and mid-sized businesses through its online and retail stores.

Carriers providing cellular network service for iPhone typically subsidize users' purchases of the device. There is no assurance that such subsidies will be continued at all or in the same amounts upon renewal of the Company's agreements with these carriers or in agreements the Company enters into with new carriers.

Many resellers have narrow operating margins and have been adversely affected in the past by weak economic conditions. Some resellers have perceived the expansion of the Company's direct sales as conflicting with their business interests as distributors and resellers of the Company's products. Such a perception could discourage resellers from investing resources in the distribution and sale of the Company's products or lead them to limit or cease distribution of those products. The Company has invested and will continue to invest in programs to enhance reseller sales, including staffing selected resellers' stores with Company employees and contractors, and improving product placement displays. These programs could require a substantial investment while providing no assurance of return or incremental revenue. The financial condition of these resellers could weaken, these resellers could stop distributing the Company's products, or uncertainty regarding demand for some or all of the Company's products could cause resellers to reduce their ordering and marketing of the Company's products.

The Company faces substantial inventory and other asset risk in addition to purchase commitment cancellation risk.

The Company records a write-down for product and component inventories that have become obsolete or exceed anticipated demand or net realizable value and accrues necessary cancellation fee reserves for orders of excess products and components. The Company also reviews its long-lived assets, including capital assets held at its suppliers' facilities and inventory prepayments, for impairment whenever events or circumstances indicate the carrying amount of an asset may not be recoverable. If the Company determines that impairment has occurred, it records a write-down equal to the amount by which the carrying value of the assets exceeds its fair value. Although the Company believes its provisions related to inventory, capital assets, inventory prepayments and other assets and purchase commitments are currently adequate, no assurance can be given that the Company will not incur additional related charges given the rapid and unpredictable pace of product obsolescence in the industries in which the Company competes.

The Company must order components for its products and build inventory in advance of product announcements and shipments. Consistent with industry practice, components are normally acquired through a combination of purchase orders, supplier contracts and open orders, in each case based on projected demand. Where appropriate, the purchases are applied to inventory component prepayments that are outstanding with the respective supplier. Purchase commitments typically cover forecasted component and manufacturing requirements for periods up to 150 days. Because the Company's markets are volatile, competitive and subject to rapid technology and price changes, there is a risk the Company will forecast incorrectly and order or produce excess or insufficient amounts of components or products, or not fully utilize firm purchase commitments.

Future operating results depend upon the Company's ability to obtain components in sufficient quantities.

Because the Company currently obtains components from single or limited sources, the Company is subject to significant supply and pricing risks. Many components, including those that are available from multiple sources, are at times subject to industry-wide shortages and significant commodity pricing fluctuations. While the Company has entered into agreements for the supply of many components, there can be no assurance that the Company will be able to extend or renew these agreements on similar terms, or at all. A number of suppliers of components may suffer from poor financial conditions, which can lead to business failure for the supplier or consolidation within a particular industry, further limiting the Company's ability to obtain sufficient quantities of components. The effects of global or regional economic conditions on the Company's suppliers, described in "*Global and regional economic conditions could materially adversely affect the Company*" above, also could affect the Company's ability to obtain components. Therefore, the Company remains subject to significant risks of supply shortages and price increases.

The Company and other participants in the markets for mobile communication and media devices and personal computers also compete for various components with other industries that have experienced increased demand for their products. The Company uses some custom components that are not common to the rest of these industries. The Company's new products often utilize custom components available from only one source. When a component or product uses new technologies, initial capacity constraints may exist until the suppliers' yields have matured or manufacturing capacity has increased. Continued availability of these components at acceptable prices, or at all, may be affected for any number of reasons, including if those suppliers decide to concentrate on the production of common components instead of components customized to meet the Company's requirements. The supply of components for a new or existing product could be delayed or constrained, or a key manufacturing vendor could delay shipments of completed products to the Company.

The Company depends on component and product manufacturing and logistical services provided by outsourcing partners, many of which are located outside of the U.S.

Substantially all of the Company's manufacturing is performed in whole or in part by a few outsourcing partners located primarily in Asia. The Company has also outsourced much of its transportation and logistics management. While these arrangements may lower operating costs, they also reduce the Company's direct control over production and distribution. It is uncertain what effect such diminished control will have on the quality or quantity of products or services, or the Company's flexibility to respond to changing conditions. Although arrangements with these partners may contain provisions for warranty expense reimbursement, the Company may remain responsible to the consumer for warranty service in the event of product defects and could experience an unanticipated product defect or warranty liability. While the Company relies on its partners to adhere to its supplier code of conduct, material violations of the supplier code of conduct could occur.

The Company relies on sole-sourced outsourcing partners in the U.S., Asia and Europe to supply and manufacture many critical components, and on outsourcing partners primarily located in Asia, for final assembly of substantially all of the Company's hardware products. Any failure of these partners to perform may have a negative impact on the Company's cost or supply of components or finished goods. In addition, manufacturing or logistics in these locations or transit to final destinations may be disrupted for a variety of reasons including, but not limited to, natural and man-made disasters, information technology system failures, commercial disputes, military actions or economic, business, labor, environmental, public health, or political issues.

The Company has invested in manufacturing process equipment, much of which is held at certain of its outsourcing partners, and has made prepayments to certain of its suppliers associated with long-term supply agreements. While these arrangements help ensure the supply of components and finished goods, if these outsourcing partners or suppliers experience severe financial problems or other disruptions in their business, such continued supply could be reduced or terminated and the net realizable value of these assets could be negatively impacted.

The Company's products and services may experience quality problems from time to time that can result in decreased sales and operating margin and harm to the Company's reputation.

The Company sells complex hardware and software products and services that can contain design and manufacturing defects. Sophisticated operating system software and applications, such as those sold by the Company, often contain "bugs" that can unexpectedly interfere with the software's intended operation. The Company's online services may from time to time experience outages, service slowdowns, or errors. Defects may also occur in components and products the Company purchases from third parties. There can be no assurance the Company will be able to detect and fix all defects in the hardware, software and services it sells. Failure to do so could result in lost revenue, significant warranty and other expenses and harm to the Company's reputation.

The Company relies on access to third-party digital content, which may not be available to the Company on commercially reasonable terms or at all.

The Company contracts with numerous third parties to offer their digital content. This includes the right to sell currently available music, movies, TV shows and books. The licensing or other distribution arrangements with these third parties are for relatively short terms and do not guarantee the continuation or renewal of these arrangements on reasonable terms, if at all. Some third-party content providers and distributors currently or in the future may offer competing products and services, and could take action to make it more difficult or impossible for the Company to license or otherwise distribute their content in the future. Other content owners, providers or distributors may seek to limit the Company's access to, or increase the cost of, such content. The Company may be unable to continue to offer a wide variety of content at reasonable prices with acceptable usage rules, or continue to expand its geographic reach. Failure to obtain the right to make available third-party digital content, or to make available such content on commercially reasonable terms, could have a material adverse impact on the Company's financial condition and operating results.

Some third-party digital content providers require the Company to provide digital rights management and other security solutions. If requirements change, the Company may have to develop or license new technology to provide these solutions. There is no assurance the Company will be able to develop or license such solutions at a reasonable cost and in a timely manner. In addition, certain countries have passed or may propose and adopt legislation that would force the Company to license its digital rights management, which could lessen the protection of content and subject it to piracy and also could negatively affect arrangements with the Company's content providers.

The Company's future performance depends in part on support from third-party software developers.

The Company believes decisions by customers to purchase its hardware products depend in part on the availability of third-party software applications and services. There is no assurance that third-party developers will continue to develop and maintain software applications and services for the Company's products. If third-party software applications and services cease to be developed and maintained for the Company's products, customers may choose not to buy the Company's products.

With respect to its Mac products, the Company believes the availability of third-party software applications and services depends in part on the developers' perception and analysis of the relative benefits of developing, maintaining and upgrading such software for the Company's products compared to Windows-based products. This analysis may be based on factors such as the market position of the Company and its products, the anticipated revenue that may be generated, expected future growth of Mac sales and the costs of developing such applications and services. If the Company's minority share of the global personal computer market causes developers to question the Mac's prospects, developers could be less inclined to develop or upgrade software for the Company's Mac products and more inclined to devote their resources to developing and upgrading software for the larger Windows market.

With respect to iOS devices, the Company relies on the continued availability and development of compelling and innovative software applications, which are distributed through a single distribution channel, the App Store. iOS devices are subject to rapid technological change, and, if third-party developers are unable to or choose not to keep up with this pace of change, third-party applications might not successfully operate and may result in dissatisfied customers. As with applications for the Company's Mac products, the availability and development of these applications also depend on developers' perceptions and analysis of the relative benefits of developing, maintaining or upgrading software for the Company's iOS devices rather than its competitors' platforms, such as Android. If developers focus their efforts on these competing platforms, the availability and quality of applications for the Company's iOS devices may suffer.

The Company relies on access to third-party intellectual property, which may not be available to the Company on commercially reasonable terms or at all.

Many of the Company's products include third-party intellectual property, which requires licenses from those third parties. Based on past experience and industry practice, the Company believes such licenses generally can be obtained on reasonable terms. There is, however, no assurance that the necessary licenses can be obtained on acceptable terms or at all. Failure to obtain the right to use third-party intellectual property, or to use such intellectual property on commercially reasonable terms, could preclude the Company from selling certain products or otherwise have a material adverse impact on the Company's financial condition and operating results.

The Company could be impacted by unfavorable results of legal proceedings, such as being found to have infringed on intellectual property rights.

The Company is subject to various legal proceedings and claims that have not yet been fully resolved and that have arisen in the ordinary course of business, and additional claims may arise in the future.

For example, technology companies, including many of the Company's competitors, frequently enter into litigation based on allegations of patent infringement or other violations of intellectual property rights. In addition, patent holding companies seek to monetize patents they have purchased or otherwise obtained. As the Company has grown, the intellectual property rights claims against it have increased and may continue to increase. In particular, the Company's cellular enabled products compete with products from mobile communication and media device companies that hold significant patent portfolios, and the number of patent claims against the Company has significantly increased. The Company is vigorously defending infringement actions in courts in a number of U.S. jurisdictions and before the U.S. International Trade Commission, as well as internationally in various countries. The plaintiffs in these actions frequently seek injunctions and substantial damages.

Regardless of the scope or validity of such patents or other intellectual property rights, or the merits of any claims by potential or actual litigants, the Company may have to engage in protracted litigation. If the Company is found to infringe one or more patents or other intellectual property rights, regardless of whether it can develop non-infringing technology, it may be required to pay substantial damages or royalties to a third-party, or it may be subject to a temporary or permanent injunction prohibiting the Company from marketing or selling certain products.

In certain cases, the Company may consider the desirability of entering into licensing agreements, although no assurance can be given that such licenses can be obtained on acceptable terms or that litigation will not occur. These licenses may also significantly increase the Company's operating expenses.

Regardless of the merit of particular claims, litigation may be expensive, time-consuming, disruptive to the Company's operations and distracting to management. In recognition of these considerations, the Company may enter into arrangements to settle litigation.

In management's opinion, there is not at least a reasonable possibility the Company may have incurred a material loss, or a material loss in excess of a recorded accrual, with respect to loss contingencies, including matters related to infringement of intellectual property rights. However, the outcome of litigation is inherently uncertain.

Although management considers the likelihood of such an outcome to be remote, if one or more legal matters were resolved against the Company in a reporting period for amounts in excess of management's expectations, the Company's consolidated financial statements for that reporting period could be materially adversely affected. Further, such an outcome could result in significant compensatory, punitive or trebled monetary damages, disgorgement of revenue or profits, remedial corporate measures or injunctive relief against the Company that could materially adversely affect its financial condition and operating results.

The Company is subject to laws and regulations worldwide, changes to which could increase the Company's costs and individually or in the aggregate adversely affect the Company's business.

The Company is subject to laws and regulations affecting its domestic and international operations in a number of areas. These U.S. and foreign laws and regulations affect the Company's activities including, but not limited to, in areas of labor, advertising, digital content, consumer protection, real estate, billing, e-commerce, promotions, quality of services, telecommunications, mobile communications and media, television, intellectual property ownership and infringement, tax, import and export requirements, anti-corruption, foreign exchange controls and cash repatriation restrictions, data privacy requirements, anti-competition, environmental, health and safety.

By way of example, laws and regulations related to mobile communications and media devices in the many jurisdictions in which the Company operates are extensive and subject to change. Such changes could include, among others, restrictions on the production, manufacture, distribution and use of devices, locking devices to a carrier's network, or mandating the use of devices on more than one carrier's network. These devices are also subject to certification and regulation by governmental and standardization bodies, as well as by cellular network carriers for use on their networks. These certification processes are extensive and time consuming, and could result in additional testing requirements, product modifications, or delays in product shipment dates, or could preclude the Company from selling certain products.

Compliance with these laws, regulations and similar requirements may be onerous and expensive, and they may be inconsistent from jurisdiction to jurisdiction, further increasing the cost of compliance and doing business. Any such costs, which may rise in the future as a result of changes in these laws and regulations or in their interpretation, could individually or in the aggregate make the Company's products and services less attractive to the Company's customers, delay the introduction of new products in one or more regions, or cause the Company to change or limit its business practices. The Company has implemented policies and procedures designed to ensure compliance with applicable laws and regulations, but there can be no assurance that the Company's employees, contractors, or agents will not violate such laws and regulations or the Company's policies and procedures.

The Company's business is subject to the risks of international operations.

The Company derives a significant portion of its revenue and earnings from its international operations. Compliance with applicable U.S. and foreign laws and regulations, such as import and export requirements, anti-corruption laws, tax laws, foreign exchange controls and cash repatriation restrictions, data privacy requirements, environmental laws, labor laws and anti-competition regulations, increases the costs of doing business in foreign jurisdictions. Although the Company has implemented policies and procedures to comply with these laws and regulations, a violation by the Company's employees, contractors, or agents could nevertheless occur. Violations of these laws and regulations could materially adversely affect the Company's brand, international growth efforts and business.

The Company also could be significantly affected by other risks associated with international activities including, but not limited to, economic and labor conditions, increased duties, taxes and other costs and political instability. Margins on sales of the Company's products in foreign countries, and on sales of products that include components obtained from foreign suppliers, could be materially adversely affected by international trade regulations, including duties, tariffs and antidumping penalties. The Company is also exposed to credit and collectability risk on its trade receivables with customers in certain international markets. There can be no assurance the Company can effectively limit its credit risk and avoid losses.

The Company's retail stores have required and will continue to require a substantial investment and commitment of resources and are subject to numerous risks and uncertainties.

The Company's retail stores have required substantial investment in equipment and leasehold improvements, information systems, inventory and personnel. The Company also has entered into substantial operating lease commitments for retail space. Certain stores have been designed and built to serve as high-profile venues to promote brand awareness and serve as vehicles for corporate sales and marketing activities. Because of their unique design elements, locations and size, these stores require substantially more investment than the Company's more typical retail stores. Due to the high cost structure associated with the Company's retail stores, a decline in sales or the closure or poor performance of individual or multiple stores could result in significant lease termination costs, write-offs of equipment and leasehold improvements and severance costs.

Many factors unique to retail operations, some of which are beyond the Company's control, pose risks and uncertainties. These risks and uncertainties include, but are not limited to, macro-economic factors that could have an adverse effect on general retail activity, as well as the Company's inability to manage costs associated with store construction and operation, the Company's failure to manage relationships with its existing retail partners, more challenging environments in managing retail operations outside the U.S., costs associated with unanticipated fluctuations in the value of retail inventory, and the Company's inability to obtain and renew leases in quality retail locations at a reasonable cost.

Investment in new business strategies and acquisitions could disrupt the Company's ongoing business and present risks not originally contemplated.

The Company has invested, and in the future may invest, in new business strategies or acquisitions. Such endeavors may involve significant risks and uncertainties, including distraction of management from current operations, greater than expected liabilities and expenses, inadequate return of capital and unidentified issues not discovered in the Company's due diligence. These new ventures are inherently risky and may not be successful.

The Company's business and reputation may be impacted by information technology system failures or network disruptions.

The Company may be subject to information technology system failures and network disruptions. These may be caused by natural disasters, accidents, power disruptions, telecommunications failures, acts of terrorism or war, computer viruses, physical or electronic break-ins, or other events or disruptions. System redundancy may be ineffective or inadequate, and the Company's disaster recovery planning may not be sufficient for all eventualities. Such failures or disruptions could, among other things, prevent access to the Company's online stores and services, preclude retail store transactions, compromise Company or customer data, and result in delayed or cancelled orders. System failures and disruptions could also impede the manufacturing and shipping of products, delivery of online services, transactions processing and financial reporting.

There may be breaches of the Company's information technology systems that materially damage business partner and customer relationships, curtail or otherwise adversely impact access to online stores and services, or subject the Company to significant reputational, financial, legal and operational consequences.

The Company's business requires it to use and store customer, employee and business partner personally identifiable information ("PII"). This may include, among other information, names, addresses, phone numbers, email addresses, contact preferences, tax identification numbers and payment account information. Although malicious attacks to gain access to PII affect many companies across various industries, the Company is at a relatively greater risk of being targeted because of its high profile and the amount of PII it manages.

The Company requires user names and passwords in order to access its information technology systems. The Company also uses encryption and authentication technologies designed to secure the transmission and storage of data and prevent access to Company data or accounts. As with all companies, these security measures are subject to third-party security breaches, employee error, malfeasance, faulty password management, or other irregularities. For example, third parties may attempt to fraudulently induce employees or customers into disclosing user names, passwords or other sensitive information, which may in turn be used to access the Company's information technology systems. To help protect customers and the Company, the Company monitors accounts and systems for unusual activity and may freeze accounts under suspicious circumstances, which may result in the delay or loss of customer orders.

The Company devotes significant resources to network security, data encryption and other security measures to protect its systems and data, but these security measures cannot provide absolute security. To the extent the Company was to experience a breach of its systems and was unable to protect sensitive data, such a breach could materially damage business partner and customer relationships, and curtail or otherwise adversely impact access to online stores and services. Moreover, if a computer security breach affects the Company's systems or results in the unauthorized release of PII, the Company's reputation and brand could be materially damaged, use of the Company's products and services could decrease, and the Company could be exposed to a risk of loss or litigation and possible liability. While the Company maintains insurance coverage that, subject to policy terms and conditions and subject to a significant self-insured retention, is designed to address certain aspects of cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in the continually evolving area of cyber risk.

The Company's business is subject to a variety of U.S. and international laws, rules, policies and other obligations regarding data protection.

The Company is subject to federal, state and international laws relating to the collection, use, retention, security and transfer of PII. In many cases, these laws apply not only to third-party transactions, but also to transfers of information between the Company and its subsidiaries, and among the Company, its subsidiaries and other parties with which the Company has commercial relations. Several jurisdictions have passed laws in this area, and other jurisdictions are considering imposing additional restrictions. These laws continue to develop and may be inconsistent from jurisdiction to jurisdiction. Complying with emerging and changing international requirements may cause the Company to incur substantial costs or require the Company to change its business practices. Noncompliance could result in penalties or significant legal liability.

The Company's privacy policy, which includes related practices concerning the use and disclosure of data, is posted on its website. Any failure by the Company, its suppliers or other parties with whom the Company does business to comply with its posted privacy policy or with other federal, state or international privacy-related or data protection laws and regulations could result in proceedings against the Company by governmental entities or others.

The Company is also subject to payment card association rules and obligations under its contracts with payment card processors. Under these rules and obligations, if information is compromised, the Company could be liable to payment card issuers for associated expenses and penalties. In addition, if the Company fails to follow payment card industry security standards, even if no customer information is compromised, the Company could incur significant fines or experience a significant increase in payment card transaction costs.

The Company's success depends largely on the continued service and availability of key personnel.

Much of the Company's future success depends on the continued availability and service of key personnel, including its Chief Executive Officer, executive team and other highly skilled employees. Experienced personnel in the technology industry are in high demand and competition for their talents is intense, especially in Silicon Valley, where most of the Company's key personnel are located.

The Company's business may be impacted by political events, war, terrorism, public health issues, natural disasters and other business interruptions.

War, terrorism, geopolitical uncertainties, public health issues and other business interruptions have caused and could cause damage or disruption to international commerce and the global economy, and thus could have a material adverse effect on the Company, its suppliers, logistics providers, manufacturing vendors and customers, including channel partners. The Company's business operations are subject to interruption by, among others, natural disasters, whether as a result of climate change or otherwise, fire, power shortages, nuclear power plant accidents, terrorist attacks and other hostile acts, labor disputes, public health issues and other events beyond its control. Such events could decrease demand for the Company's products, make it difficult or impossible for the Company to make and deliver products to its customers, including channel partners, or to receive components from its suppliers, and create delays and inefficiencies in the Company's supply chain. Should major public health issues, including pandemics, arise, the Company could be adversely affected by more stringent employee travel restrictions, additional limitations in freight services, governmental actions limiting the movement of products between regions, delays in production ramps of new products and disruptions in the operations of the Company's manufacturing vendors and component suppliers. The majority of the Company's R&D activities, its corporate headquarters, information technology systems and other critical business operations, including certain component suppliers and manufacturing vendors, are in locations that could be affected by natural disasters. In the event of a natural disaster, the Company could incur significant losses, require substantial recovery time and experience significant expenditures in order to resume operations.

The Company expects its quarterly revenue and operating results to fluctuate.

The Company's profit margins vary across its products and distribution channels. The Company's software, accessories, and service and support contracts generally have higher gross margins than certain of the Company's other products. Gross margins on the Company's hardware products vary across product lines and can change over time as a result of product transitions, pricing and configuration changes, and component, warranty, and other cost fluctuations. The Company's direct sales generally have higher associated gross margins than its indirect sales through its channel partners. In addition, the Company's gross margin and operating margin percentages, as well as overall profitability, may be materially adversely impacted as a result of a shift in product, geographic or channel mix, component cost increases, the strengthening U.S. dollar, price competition, or the introduction of new products, including those that have higher cost structures with flat or reduced pricing.

The Company has typically experienced higher net sales in its first quarter compared to other quarters due in part to seasonal holiday demand. Additionally, new product introductions can significantly impact net sales, product costs and operating expenses. Further, the Company generates a majority of its net sales from a single product and a decline in demand for that product could significantly impact quarterly net sales. The Company could also be subject to unexpected developments late in a quarter, such as lower-than-anticipated demand for the Company's products, issues with new product introductions, an internal systems failure, or failure of one of the Company's logistics, components supply, or manufacturing partners.

The Company's stock price is subject to volatility.

The Company's stock price has experienced substantial price volatility in the past and may continue to do so in the future. Additionally, the Company, the technology industry and the stock market as a whole have experienced extreme stock price and volume fluctuations that have affected stock prices in ways that may have been unrelated to these companies' operating performance. Price volatility over a given period may cause the average price at which the Company repurchases its own stock to exceed the stock's price at a given point in time. The Company believes its stock price should reflect expectations of future growth and profitability. The Company also believes its stock price should reflect expectations that its cash dividend will continue at current levels or grow and that its current share repurchase program will be fully consummated. Future dividends are subject to declaration by the Company's Board of Directors, and the Company's share repurchase program does not obligate it to acquire any specific number of shares. If the Company fails to meet expectations related to future growth, profitability, dividends, share repurchases or other market expectations, its stock price may decline significantly, which could have a material adverse impact on investor confidence and employee retention.

The Company's financial performance is subject to risks associated with changes in the value of the U.S. dollar versus local currencies.

The Company's primary exposure to movements in foreign currency exchange rates relates to non-U.S. dollar-denominated sales and operating expenses worldwide. Weakening of foreign currencies relative to the U.S. dollar adversely affects the U.S. dollar value of the Company's foreign currency-denominated sales and earnings, and generally leads the Company to raise international pricing, potentially reducing demand for the Company's products. Margins on sales of the Company's products in foreign countries and on sales of products that include components obtained from foreign suppliers, could be materially adversely affected by foreign currency exchange rate fluctuations. In some circumstances, for competitive or other reasons, the Company may decide not to raise local prices to fully offset the dollar's strengthening, or at all, which would adversely affect the U.S. dollar value of the Company's foreign currency-denominated sales and earnings. Conversely, a strengthening of foreign currencies relative to the U.S. dollar, while generally beneficial to the Company's foreign currency-denominated sales and earnings, could cause the Company to reduce international pricing and incur losses on its foreign currency derivative instruments, thereby limiting the benefit. Additionally, strengthening of foreign currencies may also increase the Company's cost of product components denominated in those currencies, thus adversely affecting gross margins.

The Company uses derivative instruments, such as foreign currency forward and option contracts, to hedge certain exposures to fluctuations in foreign currency exchange rates. The use of such hedging activities may not offset any, or more than a portion, of the adverse financial effects of unfavorable movements in foreign exchange rates over the limited time the hedges are in place.

The Company is exposed to credit risk and fluctuations in the market values of its investment portfolio.

Given the global nature of its business, the Company has both domestic and international investments. Credit ratings and pricing of the Company's investments can be negatively affected by liquidity, credit deterioration, financial results, economic risk, political risk, sovereign risk or other factors. As a result, the value and liquidity of the Company's cash, cash equivalents and marketable securities may fluctuate substantially. Therefore, although the Company has not realized any significant losses on its cash, cash equivalents and marketable securities, future fluctuations in their value could result in a significant realized loss.

The Company is exposed to credit risk on its trade accounts receivable, vendor non-trade receivables and prepayments related to long-term supply agreements, and this risk is heightened during periods when economic conditions worsen.

The Company distributes its products through third-party cellular network carriers, wholesalers, retailers and value-added resellers. The Company also sells its products directly to small and mid-sized businesses and education, enterprise and government customers. A substantial majority of the Company's outstanding trade receivables are not covered by collateral, third-party financing arrangements or credit insurance. The Company's exposure to credit and collectability risk on its trade receivables is higher in certain international markets and its ability to mitigate such risks may be limited. The Company also has unsecured vendor non-trade receivables resulting from purchases of components by outsourcing partners and other vendors that manufacture sub-assemblies or assemble final products for the Company. In addition, the Company has made prepayments associated with long-term supply agreements to secure supply of inventory components. As of September 26, 2015, a significant portion of the Company's trade receivables was concentrated within cellular network carriers, and its vendor non-trade receivables and prepayments related to long-term supply agreements were concentrated among a few individual vendors located primarily in Asia. While the Company has procedures to monitor and limit exposure to credit risk on its trade and vendor non-trade receivables, as well as long-term prepayments, there can be no assurance such procedures will effectively limit its credit risk and avoid losses.

The Company could be subject to changes in its tax rates, the adoption of new U.S. or international tax legislation or exposure to additional tax liabilities.

The Company is subject to taxes in the U.S. and numerous foreign jurisdictions, including Ireland, where a number of the Company's subsidiaries are organized. Due to economic and political conditions, tax rates in various jurisdictions may be subject to significant change. The Company's effective tax rates could be affected by changes in the mix of earnings in countries with differing statutory tax rates, changes in the valuation of deferred tax assets and liabilities, or changes in tax laws or their interpretation, including in the U.S. and Ireland. For example, in June 2014, the European Commission opened a formal investigation of Ireland to examine whether decisions by the tax authorities with regard to the corporate income tax to be paid by two of the Company's Irish subsidiaries comply with European Union rules on state aid. If the European Commission were to conclude against Ireland, it could require Ireland to recover from the Company past taxes covering a period of up to 10 years reflective of the disallowed state aid, and such amount could be material.

The Company is also subject to the examination of its tax returns and other tax matters by the Internal Revenue Service and other tax authorities and governmental bodies. The Company regularly assesses the likelihood of an adverse outcome resulting from these examinations to determine the adequacy of its provision for taxes. There can be no assurance as to the outcome of these examinations. If the Company's effective tax rates were to increase, particularly in the U.S. or Ireland, or if the ultimate determination of the Company's taxes owed is for an amount in excess of amounts previously accrued, the Company's financial condition, operating results and cash flows could be adversely affected.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

The Company's headquarters are located in Cupertino, California. As of September 26, 2015, the Company owned or leased 25.6 million square feet of building space, primarily in the U.S. The Company also owned or leased building space in various locations, including throughout Europe, China, Singapore and Japan. Of the total owned or leased building space 18.5 million square feet was leased building space, which includes approximately 5.3 million square feet related to retail store space. Additionally, the Company owns a total of 1,757 acres of land in various locations.

As of September 26, 2015, the Company owned a manufacturing facility in Cork, Ireland that also housed a customer support call center; facilities in Elk Grove, California that included warehousing and distribution operations and a customer support call center; and a facility in Mesa, Arizona. The Company also owned land in Austin, Texas where it is expanding its existing office space and customer support call center. In addition, the Company owned facilities and land for R&D and corporate functions in San Jose, California and Cupertino, California, including land that is being developed for the Company's second corporate campus. The Company also owned data centers in Newark, California; Maiden, North Carolina; Prineville, Oregon; and Reno, Nevada. Outside the U.S., the Company owned additional facilities for various purposes.

The Company believes its existing facilities and equipment, which are used by all operating segments, are in good operating condition and are suitable for the conduct of its business. The Company has invested in internal capacity and strategic relationships with outside manufacturing vendors and continues to make investments in capital equipment as needed to meet anticipated demand for its products.

Item 3. Legal Proceedings

The Company is subject to the legal proceedings and claims discussed below as well as certain other legal proceedings and claims that have not been fully resolved and that have arisen in the ordinary course of business. In the opinion of management, there was not at least a reasonable possibility the Company may have incurred a material loss, or a material loss in excess of a recorded accrual, with respect to loss contingencies for asserted legal and other claims. However, the outcome of legal proceedings and claims brought against the Company is subject to significant uncertainty. Therefore, although management considers the likelihood of such an outcome to be remote, if one or more of these legal matters were resolved against the Company in a reporting period for amounts in excess of management's expectations, the Company's consolidated financial statements for that reporting period could be materially adversely affected. See the risk factor "*The Company could be impacted by unfavorable results of legal proceedings, such as being found to have infringed on intellectual property rights*" in Part I, Item 1A of this Form 10-K under the heading "Risk Factors." The Company settled certain matters during the fourth quarter of 2015 that did not individually or in the aggregate have a material impact on the Company's financial condition or operating results.

Apple eBooks Antitrust Litigation (United States of America v. Apple Inc., et al.)

On April 11, 2012, the U.S. Department of Justice filed a civil antitrust action against the Company and five major book publishers in the U.S. District Court for the Southern District of New York, alleging an unreasonable restraint of interstate trade and commerce in violation of §1 of the Sherman Act and seeking, among other things, injunctive relief, the District Court's declaration that the Company's agency agreements with the publishers are null and void and/or the District Court's reformation of such agreements. On July 10, 2013, the District Court found, following a bench trial, that the Company conspired to restrain trade in violation of §1 of the Sherman Act and relevant state statutes to the extent those laws are congruent with §1 of the Sherman Act. The District Court entered a permanent injunction, which took effect on October 6, 2013 and will be in effect for five years unless the judgment is overturned on appeal. The Company has taken the necessary steps to comply with the terms of the District Court's order, including renegotiating agreements with the five major eBook publishers, updating its antitrust training program and completing a two-year monitorship with a court-appointed antitrust compliance monitor, whose appointment the District Court ended in October 2015. The Company appealed the District Court's decision. Pursuant to a settlement agreement reached in June 2014, any damages the Company may be obligated to pay will be determined by the outcome of the final adjudication following exhaustion of all appeals.

Item 4. Mine Safety Disclosures

Not applicable.

PART II

Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

The Company's common stock is traded on the NASDAQ Stock Market LLC ("NASDAQ") under the symbol AAPL.

Price Range of Common Stock

The price range per share of common stock presented below represents the highest and lowest intraday sales prices for the Company's common stock on the NASDAQ during each quarter of the two most recent years.

	Fourth Quarter	Third Quarter	Second Quarter	First Quarter
2015 price range per share	$ 132.97 - $ 92.00	$ 134.54 - $ 123.10	$ 133.60 - $ 104.63	$ 119.75 - $ 95.18
2014 price range per share	$ 103.74 - $ 92.09	$ 95.05 - $ 73.05	$ 80.18 - $ 70.51	$ 82.16 - $ 67.77

Holders

As of October 9, 2015, there were 25,924 shareholders of record.

Dividends

The Company paid a total of $11.4 billion and $11.0 billion in dividends during 2015 and 2014, respectively, and expects to pay quarterly dividends of $0.52 per common share each quarter, subject to declaration by the Board of Directors. The Company also plans to increase its dividend on an annual basis, subject to declaration by the Board of Directors.

Purchases of Equity Securities by the Issuer and Affiliated Purchasers

Share repurchase activity during the three months ended September 26, 2015 was as follows (in millions, except number of shares, which are reflected in thousands, and per share amounts):

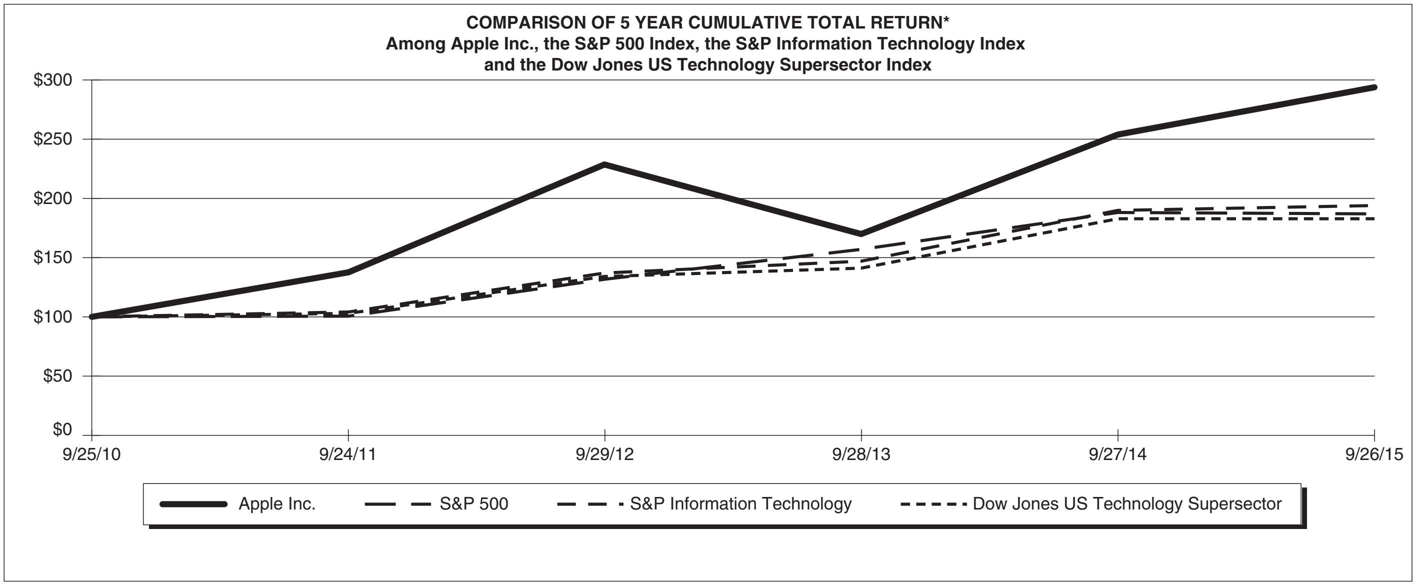
Periods	Total Number of Shares Purchased	Average Price Paid Per Share	Total Number of Shares Purchased as Part of Publicly Announced Plans or Programs	Approximate Dollar Value of Shares That May Yet Be Purchased Under the Plans or Programs [1]
June 28, 2015 to August 1, 2015:				
May 2015 ASR	9,973 [2]	[2]	9,973 [2]	
Open market and privately negotiated purchases	15,882	$ 124.66	15,882	
August 2, 2015 to August 29, 2015:				
Open market and privately negotiated purchases	68,526	$ 114.15	68,526	
August 30, 2015 to September 26, 2015:				
Open market and privately negotiated purchases	37,394	$ 112.94	37,394	
Total	131,775			$ 36,024

[1] In 2012, the Company's Board of Directors authorized a program to repurchase up to $10 billion of the Company's common stock beginning in 2013. The Company's Board of Directors increased the authorization to repurchase the Company's common stock to $60 billion in April 2013, to $90 billion in April 2014 and to $140 billion in April 2015. As of September 26, 2015, $104 billion of the $140 billion had been utilized. The remaining $36 billion in the table represents the amount available to repurchase shares under the authorized repurchase program as of September 26, 2015. The Company's share repurchase program does not obligate it to acquire any specific number of shares. Under the program, shares may be repurchased in privately negotiated and/or open market transactions, including under plans complying with Rule 10b5-1 under the Exchange Act.

[2] In May 2015, the Company entered into an accelerated share repurchase arrangement ("ASR") to purchase up to $6.0 billion of the Company's common stock. In July 2015, the purchase period for this ASR ended and an additional 10.0 million shares were delivered and retired. In total, 48.3 million net shares were delivered under this ASR at an average repurchase price of $124.24.

Company Stock Performance

The following graph shows a comparison of cumulative total shareholder return, calculated on a dividend reinvested basis, for the Company, the S&P 500 Index, the S&P Information Technology Index and the Dow Jones U.S. Technology Supersector Index for the five years ended September 26, 2015. The graph assumes $100 was invested in each of the Company's common stock, the S&P 500 Index, the S&P Information Technology Index and the Dow Jones U.S. Technology Supersector Index as of the market close on September 24, 2010. Note that historic stock price performance is not necessarily indicative of future stock price performance.



* $100 invested on 9/25/10 in stock or index, including reinvestment of dividends. Data points are the last day of each fiscal year for the Company's common stock and September 30th for indexes.

	September 2010	September 2011	September 2012	September 2013	September 2014	September 2015
Apple Inc.	$ 100	$ 138	$ 229	$ 170	$ 254	$ 294
S&P 500 Index	$ 100	$ 101	$ 132	$ 157	$ 188	$ 187
S&P Information Technology Index	$ 100	$ 104	$ 137	$ 147	$ 190	$ 194
Dow Jones U.S. Technology Supersector Index	$ 100	$ 103	$ 134	$ 141	$ 183	$ 183

Item 6. Selected Financial Data

The information set forth below for the five years ended September 26, 2015, is not necessarily indicative of results of future operations, and should be read in conjunction with Part II, Item 7, “Management’s Discussion and Analysis of Financial Condition and Results of Operations” and the consolidated financial statements and related notes thereto included in Part II, Item 8 of this Form 10-K to fully understand factors that may affect the comparability of the information presented below (in millions, except number of shares, which are reflected in thousands, and per share amounts).

	2015	2014	2013	2012	2011
Net sales	$ 233,715	$ 182,795	$ 170,910	$ 156,508	$ 108,249
Net income	$ 53,394	$ 39,510	$ 37,037	$ 41,733	$ 25,922
Earnings per share:					
Basic	$ 9.28	$ 6.49	$ 5.72	$ 6.38	$ 4.01
Diluted	$ 9.22	$ 6.45	$ 5.68	$ 6.31	$ 3.95
Cash dividends declared per share	$ 1.98	$ 1.82	$ 1.64	$ 0.38	$ 0
Shares used in computing earnings per share:					
Basic	5,753,421	6,085,572	6,477,320	6,543,726	6,469,806
Diluted	5,793,069	6,122,663	6,521,634	6,617,483	6,556,514
Total cash, cash equivalents and marketable securities	$ 205,666	$ 155,239	$ 146,761	$ 121,251	$ 81,570
Total assets	$ 290,479	$ 231,839	$ 207,000	$ 176,064	$ 116,371
Commercial paper	$ 8,499	$ 6,308	$ 0	$ 0	$ 0
Total term debt [2]	$ 55,963	$ 28,987	$ 16,960	$ 0	$ 0
Other long-term obligations [1]	$ 33,427	$ 24,826	$ 20,208	$ 16,664	$ 10,100
Total liabilities	$ 171,124	$ 120,292	$ 83,451	$ 57,854	$ 39,756
Total shareholders’ equity	$ 119,355	$ 111,547	$ 123,549	$ 118,210	$ 76,615

[1] Other long-term obligations exclude non-current deferred revenue.

[2] Includes current and long-term portion of term debt.

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

This section and other parts of this Annual Report on Form 10-K ("Form 10-K") contain forward-looking statements, within the meaning of the Private Securities Litigation Reform Act of 1995, that involve risks and uncertainties. Forward-looking statements provide current expectations of future events based on certain assumptions and include any statement that does not directly relate to any historical or current fact. Forward-looking statements can also be identified by words such as "future," "anticipates," "believes," "estimates," "expects," "intends," "plans," "predicts," "will," "would," "could," "can," "may," and similar terms. Forward-looking statements are not guarantees of future performance and the Company's actual results may differ significantly from the results discussed in the forward-looking statements. Factors that might cause such differences include, but are not limited to, those discussed in Part I, Item 1A of this Form 10-K under the heading "Risk Factors," which are incorporated herein by reference. The following discussion should be read in conjunction with the consolidated financial statements and notes thereto included in Part II, Item 8 of this Form 10-K. All information presented herein is based on the Company's fiscal calendar. Unless otherwise stated, references to particular years, quarters, months or periods refer to the Company's fiscal years ended in September and the associated quarters, months and periods of those fiscal years. Each of the terms the "Company" and "Apple" as used herein refers collectively to Apple Inc. and its wholly-owned subsidiaries, unless otherwise stated. The Company assumes no obligation to revise or update any forward-looking statements for any reason, except as required by law.

Overview and Highlights

The Company designs, manufactures and markets mobile communication and media devices, personal computers and portable digital music players, and sells a variety of related software, services, accessories, networking solutions and third-party digital content and applications. The Company sells its products worldwide through its retail stores, online stores and direct sales force, as well as through third-party cellular network carriers, wholesalers, retailers and value-added resellers. In addition, the Company sells a variety of third-party Apple compatible products, including application software and various accessories through its online and retail stores. The Company sells to consumers, small and mid-sized businesses and education, enterprise and government customers.

Fiscal 2015 Highlights

Net sales rose 28% or $50.9 billion during 2015 compared to 2014, driven by a 52% year-over-year increase in iPhone® net sales. iPhone net sales and unit sales in 2015 increased in all of the Company's reportable operating segments. The Company also experienced year-over-year net sales increases in Mac®, Services and Other Products. Apple Watch®, which launched during the third quarter of 2015, accounted for more than 100% of the year-over-year growth in net sales of Other Products. Net sales growth during 2015 was partially offset by the effect of weakness in most foreign currencies relative to the U.S. dollar and lower iPad® net sales. Total net sales increased in each of the Company's reportable operating segments, with particularly strong growth in Greater China where year-over-year net sales increased 84%.

In April 2015, the Company announced a significant increase to its capital return program by raising the expected total size of the program to $200 billion through March 2017. This included increasing its share repurchase authorization to $140 billion and raising its quarterly dividend to $0.52 per share beginning in May 2015. During 2015, the Company spent $36.0 billion to repurchase shares of its common stock and paid dividends and dividend equivalents of $11.6 billion. Additionally, the Company issued $14.5 billion of U.S. dollar-denominated, €4.8 billion of euro-denominated, SFr1.3 billion of Swiss franc-denominated, £1.3 billion of British pound-denominated, A$2.3 billion of Australian dollar-denominated and ¥250.0 billion of Japanese yen-denominated term debt during 2015.

Fiscal 2014 Highlights

Net sales rose 7% or $11.9 billion during 2014 compared to 2013. This was driven by increases in net sales of iPhone, Mac and Services. Net sales and unit sales increased for iPhone primarily due to the successful introduction of iPhone 5s and 5c in the latter half of calendar year 2013, the successful launch of iPhone 6 and 6 Plus beginning in the fourth quarter of 2014, and expanded distribution. Mac net sales and unit sales increased primarily due to strong demand for MacBook Air® and MacBook Pro® which were updated in 2014 with faster processors and offered at lower prices. Net sales of Services grew primarily due to increased revenue from sales through the App Store®, AppleCare® and licensing. Growth in these areas was partially offset by the year-over-year decline in net sales for iPad due to lower unit sales in many markets, and a decline in net sales of Other Products. All of the Company's operating segments other than the Rest of Asia Pacific segment experienced increased net sales in 2014, with growth being strongest in the Greater China and Japan operating segments.

During 2014, the Company completed various business acquisitions, including the acquisitions of Beats Music, LLC, which offers a subscription streaming music service, and Beats Electronics, LLC, which makes Beats® headphones, speakers and audio software.

In April 2014, the Company increased its share repurchase authorization to $90 billion and the quarterly dividend was raised to $0.47 per common share, resulting in an overall increase in its capital return program from $100 billion to over $130 billion. During 2014, the Company utilized $45 billion to repurchase its common stock and paid dividends and dividend equivalents of $11.1 billion. The Company also issued $12.0 billion of long-term debt during 2014, with varying maturities through 2044, and launched a commercial paper program, with $6.3 billion outstanding as of September 27, 2014.

Sales Data

The following table shows net sales by operating segment and net sales and unit sales by product during 2015, 2014 and 2013 (dollars in millions and units in thousands):

	2015	Change	2014	Change	2013
Net Sales by Operating Segment:					
Americas	$ 93,864	17%	$ 80,095	4%	$ 77,093
Europe	50,337	14%	44,285	8%	40,980
Greater China	58,715	84%	31,853	18%	27,016
Japan	15,706	3%	15,314	11%	13,782
Rest of Asia Pacific	15,093	34%	11,248	(7)%	12,039
Total net sales	$ 233,715	28%	$ 182,795	7%	$ 170,910
Net Sales by Product:					
iPhone [1]	$ 155,041	52%	$ 101,991	12%	$ 91,279
iPad [1]	23,227	(23)%	30,283	(5)%	31,980
Mac [1]	25,471	6%	24,079	12%	21,483
Services [2]	19,909	10%	18,063	13%	16,051
Other Products [1][3]	10,067	20%	8,379	(17)%	10,117
Total net sales	$ 233,715	28%	$ 182,795	7%	$ 170,910
Unit Sales by Product:					
iPhone	231,218	37%	169,219	13%	150,257
iPad	54,856	(19)%	67,977	(4)%	71,033
Mac	20,587	9%	18,906	16%	16,341

[1] Includes deferrals and amortization of related software upgrade rights and non-software services.

[2] Includes revenue from the iTunes Store®, App Store, Mac App Store, iBooks Store™ and Apple Music™ (collectively "Internet Services"), AppleCare, Apple Pay®, licensing and other services.

[3] Includes sales of Apple TV®, Apple Watch, Beats products, iPod and Apple-branded and third-party accessories.

Product Performance

iPhone

The following table presents iPhone net sales and unit sales information for 2015, 2014 and 2013 (dollars in millions and units in thousands):

	2015	Change	2014	Change	2013
Net sales	$ 155,041	52%	$ 101,991	12%	$ 91,279
Percentage of total net sales	66%		56%		53%
Unit sales	231,218	37%	169,219	13%	150,257

The year-over-year growth in iPhone net sales and unit sales during 2015 primarily resulted from strong demand for iPhone 6 and 6 Plus during 2015. Overall average selling prices ("ASPs") for iPhone increased by 11% during 2015 compared to 2014, due primarily to the introduction of iPhone 6 and 6 Plus in September 2014, partially offset by the effect of weakness in most foreign currencies relative to the U.S. dollar.

The year-over-year growth in iPhone net sales and unit sales in 2014 resulted primarily from the successful introduction of new iPhones in the latter half of calendar year 2013, the successful launch of iPhone 6 and 6 Plus beginning in September 2014, and expanded distribution. iPhone unit sales grew in all of the Company's operating segments, while iPhone net sales grew in all segments except Rest of Asia Pacific. Overall ASPs for iPhone were relatively flat in 2014 compared to 2013, with growth in ASPs in the Americas segment being offset by a decline in ASPs in the Greater China, Japan and Rest of Asia Pacific segments.

iPad

The following table presents iPad net sales and unit sales information for 2015, 2014 and 2013 (dollars in millions and units in thousands):

	2015	Change	2014	Change	2013
Net sales	$ 23,227	(23)%	$ 30,283	(5)%	$ 31,980
Percentage of total net sales	10%		17%		19%
Unit sales	54,856	(19)%	67,977	(4)%	71,033

Net sales and unit sales for iPad declined during 2015 compared to 2014. The Company believes the decline in iPad sales is due in part to a longer repurchase cycle for iPads and some level of cannibalization from the Company's other products. iPad ASPs declined by 5% during 2015 compared to 2014, primarily as a result of the effect of weakness in most foreign currencies relative to the U.S. dollar and a shift in mix to lower-priced iPads.

Net sales and unit sales for iPad declined in 2014 compared to 2013. iPad net sales and unit sales grew in the Greater China and Japan segments but this growth was more than offset by a decline in all other segments. Overall iPad ASPs were relatively flat in 2014 compared to 2013 with a shift in mix to higher-priced iPads being offset by the October 2013 price reduction of iPad mini™. ASPs increased in the Japan and Rest of Asia Pacific segments but were slightly down in other segments.

Mac

The following table presents Mac net sales and unit sales information for 2015, 2014 and 2013 (dollars in millions and units in thousands):

	2015	Change	2014	Change	2013
Net sales	$ 25,471	6%	$ 24,079	12%	$ 21,483
Percentage of total net sales	11%		13%		13%
Unit sales	20,587	9%	18,906	16%	16,341

The year-over-year growth in Mac net sales and unit sales during 2015 was driven by strong demand for Mac portables. Mac ASPs declined 3% during 2015 compared to 2014 largely due to the effect of weakness in most foreign currencies relative to the U.S. dollar.

The year-over-year growth in Mac net sales and unit sales for 2014 was primarily driven by increased sales of MacBook Air, MacBook Pro and Mac Pro. Mac net sales and unit sales increased in all of the Company's operating segments. Mac ASPs decreased during 2014 compared to 2013 primarily due to price reductions on certain Mac models and a shift in mix towards Mac portable systems.

Services

The following table presents net sales information of Services for 2015, 2014 and 2013 (dollars in millions):

	2015	Change	2014	Change	2013
Net sales	$ 19,909	10%	$ 18,063	13%	$ 16,051
Percentage of total net sales	9%		10%		9%

The increase in net sales of Services during 2015 compared to 2014 was primarily due to growth from Internet Services and licensing. The App Store, included within Internet Services, generated strong year-over-year net sales growth of 29%.

The increase in net sales of Services in 2014 compared to 2013 was primarily due to growth in net sales from Internet Services, AppleCare and licensing. Internet Services generated a total of $10.2 billion in net sales during 2014 compared to $9.3 billion during 2013. Growth in net sales from Internet Services was driven by increases in revenue from app sales reflecting continued growth in the installed base of iOS devices and the expanded offerings of iOS apps and related in-app purchases. This was partially offset by a decline in sales of digital music.

Segment Operating Performance

The Company manages its business primarily on a geographic basis. The Company's reportable operating segments consist of the Americas, Europe, Greater China, Japan and Rest of Asia Pacific. The Americas segment includes both North and South America. The Europe segment includes European countries, as well as India, the Middle East and Africa. The Greater China segment includes China, Hong Kong and Taiwan. The Rest of Asia Pacific segment includes Australia and those Asian countries not included in the Company's other reportable operating segments. Although, each reportable operating segment provides similar hardware and software products and similar services, they are managed separately to better align with the location of the Company's customers and distribution partners and the unique market dynamics of each geographic region. Further information regarding the Company's reportable operating segments can be found in Part II, Item 8 of this Form 10-K in the Notes to Consolidated Financial Statements in Note 11, "Segment Information and Geographic Data."

Americas

The following table presents Americas net sales information for 2015, 2014 and 2013 (dollars in millions):

	2015	Change	2014	Change	2013
Net sales	$ 93,864	17%	$ 80,095	4%	$ 77,093
Percentage of total net sales	40%		44%		45%

The year-over-year growth in Americas net sales during 2015 was driven primarily by growth in net sales and unit sales of iPhone, partially offset by a decline in net sales and unit sales of iPad.

The growth in the Americas segment in 2014 was due to increased net sales of iPhone, Mac and Services that was partially offset by a decline in net sales of iPad and Other Products and weakness in foreign currencies relative to the U.S. dollar compared to 2013. iPhone growth resulted primarily from the successful introduction of iPhone 5s and 5c in September 2013 and the successful launch of iPhone 6 and 6 Plus in September 2014. Mac growth was driven primarily by increased net sales and unit sales of MacBook Air and Mac Pro.

Europe

The following table presents Europe net sales information for 2015, 2014 and 2013 (dollars in millions):

	2015	Change	2014	Change	2013
Net sales	$ 50,337	14%	$ 44,285	8%	$ 40,980
Percentage of total net sales	22%		24%		24%

The year-over-year increase in Europe net sales during 2015 was driven primarily by growth in net sales and unit sales of iPhone, partially offset by the effect of weakness in foreign currencies relative to the U.S. dollar and a decline in net sales and unit sales of iPad.

The growth in the Europe segment in 2014 was due to increased net sales of iPhone, Mac and Services, as well as strength in European currencies relative to the U.S. dollar, partially offset by a decline in net sales of iPad. iPhone growth resulted primarily from the successful introduction of iPhone 5s and 5c in the second half of calendar 2013 and the successful launch of iPhone 6 and 6 Plus in over 20 countries in Europe in September 2014. Mac growth was driven primarily by increased net sales and unit sales of MacBook Air, MacBook Pro and Mac Pro.

Greater China

The following table presents Greater China net sales information for 2015, 2014 and 2013 (dollars in millions):

	2015	Change	2014	Change	2013
Net sales	$ 58,715	84%	$ 31,853	18%	$ 27,016
Percentage of total net sales	25%		17%		16%

Greater China experienced strong year-over-year increases in net sales during 2015 driven primarily by iPhone sales.

The Greater China segment experienced year-over-year growth in net sales in 2014 that was significantly higher than the growth rate for the Company overall. Greater China growth was driven by higher unit sales and net sales of all major product categories, in addition to higher net sales of Services. Growth in net sales and unit sales of iPhone was especially strong, driven by the successful launch of iPhone 5s and 5c in Mainland China and Hong Kong in September 2013, the successful launch of iPhone 6 and 6 Plus in Hong Kong in September 2014, increased demand for the Company’s entry-priced iPhones and the addition of a significant new carrier in the second quarter of 2014.

Japan

The following table presents Japan net sales information for 2015, 2014 and 2013 (dollars in millions):

	2015	Change	2014	Change	2013
Net sales	$ 15,706	3%	$ 15,314	11%	$ 13,782
Percentage of total net sales	7%		8%		8%

The year-over-year increase in Japan net sales during 2015 was driven primarily by growth in Services largely associated with strong App Store sales, partially offset by the effect of weakness in the Japanese yen relative to the U.S. dollar.

In 2014 the Japan segment generated year-over-year increases in net sales and unit sales of every major product category and experienced growth in net sales of Services. The year-over-year growth in iPhone was driven by the successful launch of iPhone 5s and 5c in September 2013, the successful launch of iPhone 6 and 6 Plus in September 2014, increased demand for the Company’s entry-priced iPhones and the addition of a significant new carrier in the fourth quarter of 2013. These positive factors were partially offset by weakness in the Japanese Yen relative to the U.S. dollar.

Rest of Asia Pacific

The following table presents Rest of Asia Pacific net sales information for 2015, 2014 and 2013 (dollars in millions):

	2015	Change	2014	Change	2013
Net sales	$ 15,093	34%	$ 11,248	(7)%	$ 12,039
Percentage of total net sales	6%		6%		7%

The year-over-year increase in Rest of Asia Pacific net sales during 2015 primarily reflects strong growth in net sales and unit sales of iPhone, partially offset by the effect of weakness in foreign currencies relative to the U.S. dollar and a decline in net sales and unit sales of iPad.

Net sales in the Rest of Asia Pacific segment declined in 2014 compared to 2013 due to year-over-year reductions in net sales in all major product categories except Mac and reductions in unit sales of iPad. Net sales in 2014 were also negatively affected by the weakness in several foreign currencies relative to the U.S. dollar, including the Australian dollar.

Gross Margin

Gross margin for 2015, 2014 and 2013 is as follows (dollars in millions):

	2015	2014	2013
Net sales	$ 233,715	$ 182,795	$ 170,910
Cost of sales	140,089	112,258	106,606
Gross margin	$ 93,626	$ 70,537	$ 64,304
Gross margin percentage	40.1%	38.6%	37.6%

The year-over-year increase in the gross margin percentage in 2015 was driven primarily by a favorable shift in mix to products with higher margins and, to a lesser extent, by improved leverage on fixed costs from higher net sales. These positive factors were partially offset primarily by higher product cost structures and, to a lesser extent, by the effect of weakness in most foreign currencies relative to the U.S. dollar.

The year-over-year increase in the gross margin percentage in 2014 was driven by multiple factors including lower commodity costs, a favorable shift in mix to products with higher margins and improved leverage on fixed costs from higher net sales, which was partially offset by the weakness in several foreign currencies relative to the U.S. dollar, price reductions on select products and higher cost structures on certain new products.

The Company anticipates gross margin during the first quarter of 2016 to be between 39% and 40%. The foregoing statement regarding the Company’s expected gross margin percentage in the first quarter of 2016 is forward-looking and could differ from actual results. The Company’s future gross margins can be impacted by multiple factors including, but not limited to, those set forth in Part I, Item 1A of this Form 10-K under the heading “Risk Factors” and those described in this paragraph. In general, the Company believes gross margins will remain under downward pressure due to a variety of factors, including continued industry wide global product pricing pressures, increased competition, compressed product life cycles, product transitions, potential increases in the cost of components, and potential strengthening of the U.S. dollar, as well as potential increases in the costs of outside manufacturing services and a potential shift in the Company’s sales mix towards products with lower gross margins. In response to competitive pressures, the Company expects it will continue to take product pricing actions, which would adversely affect gross margins. Gross margins could also be affected by the Company’s ability to manage product quality and warranty costs effectively and to stimulate demand for certain of its products. Due to the Company’s significant international operations, its financial condition and operating results, including gross margins, could be significantly affected by fluctuations in exchange rates.

Operating Expenses

Operating expenses for 2015, 2014 and 2013 are as follows (dollars in millions):

	2015	Change	2014	Change	2013
Research and development	$ 8,067	34%	$ 6,041	35%	$ 4,475
Percentage of total net sales	3%		3%		3%
Selling, general and administrative	$ 14,329	19%	$ 11,993	11%	$ 10,830
Percentage of total net sales	6%		7%		6%
Total operating expenses	$ 22,396	24%	$ 18,034	18%	$ 15,305
Percentage of total net sales	10%		10%		9%

Research and Development

The year-over-year growth in R&D expense in 2015 and 2014 was driven primarily by an increase in headcount and related expenses, including share-based compensation costs, and material costs to support expanded R&D activities. The Company continues to believe that focused investments in R&D are critical to its future growth and competitive position in the marketplace and are directly related to timely development of new and updated products that are central to the Company’s core business strategy.

Selling, General and Administrative

The year-over-year growth in selling, general and administrative expense in 2015 and 2014 was primarily due to increased headcount and related expenses, including share-based compensation costs, and higher spending on marketing and advertising.

Other Income/(Expense), Net

Other income/(expense), net for 2015, 2014 and 2013 are as follows (dollars in millions):

	2015	Change	2014	Change	2013
Interest and dividend income	$ 2,921		$ 1,795		$ 1,616
Interest expense	(733)		(384)		(136)
Other expense, net	(903)		(431)		(324)
Total other income/(expense), net	$ 1,285	31%	$ 980	(15)%	$ 1,156

The increase in other income/(expense), net during 2015 compared to 2014 was due primarily to higher interest income, partially offset by higher expenses associated with foreign exchange activity and higher interest expense on debt. The decrease in other income and expense during 2014 compared to 2013 was due primarily to higher interest expense on debt and higher expenses associated with foreign exchange rate movements, partially offset by lower premium expenses on foreign exchange contracts and higher interest income. The weighted-average interest rate earned by the Company on its cash, cash equivalents and marketable securities was 1.49%, 1.11% and 1.03% in 2015, 2014 and 2013, respectively.

Provision for Income Taxes

Provision for income taxes and effective tax rates for 2015, 2014 and 2013 are as follows (dollars in millions):

	2015	2014	2013
Provision for income taxes	$ 19,121	$ 13,973	$ 13,118
Effective tax rate	26.4%	26.1%	26.2%

The Company's effective tax rates for 2015, 2014 and 2013 differ from the statutory federal income tax rate of 35% due primarily to certain undistributed foreign earnings, a substantial portion of which was generated by subsidiaries organized in Ireland, for which no U.S. taxes are provided when such earnings are intended to be indefinitely reinvested outside the U.S. The higher effective tax rate during 2015 compared to 2014 was due primarily to higher foreign taxes. The effective tax rate in 2014 compared to 2013 was relatively flat.

As of September 26, 2015, the Company had deferred tax assets arising from deductible temporary differences, tax losses and tax credits of $7.8 billion and deferred tax liabilities of $24.1 billion. Management believes it is more likely than not that forecasted income, including income that may be generated as a result of certain tax planning strategies, together with future reversals of existing taxable temporary differences, will be sufficient to fully recover the deferred tax assets. The Company will continue to evaluate the realizability of deferred tax assets quarterly by assessing the need for and the amount of a valuation allowance.

The U.S. Internal Revenue Service is currently examining the years 2010 through 2012, and all years prior to 2010 are closed. In addition, the Company is subject to audits by state, local and foreign tax authorities. In major states and major foreign jurisdictions, the years subsequent to 2003 generally remain open and could be subject to examination by the taxing authorities. Management believes that adequate provisions have been made for any adjustments that may result from tax examinations. However, the outcome of tax audits cannot be predicted with certainty. If any issues addressed in the Company's tax audits are resolved in a manner not consistent with management's expectations, the Company could be required to adjust its provision for income taxes in the period such resolution occurs.

On June 11, 2014, the European Commission issued an opening decision initiating a formal investigation against Ireland for alleged state aid to the Company. The opening decision concerns the allocation of profits for taxation purposes of the Irish branches of two subsidiaries of the Company. The Company believes the European Commission's assertions are without merit. If the European Commission were to conclude against Ireland, the European Commission could require Ireland to recover from the Company past taxes covering a period of up to 10 years reflective of the disallowed state aid. While such amount could be material, as of September 26, 2015 the Company is unable to estimate the impact.

Recent Accounting Pronouncements

In May 2014, the Financial Accounting Standards Board ("FASB") issued Accounting Standards Update ("ASU") No. 2014-09, Revenue from Contracts with Customers (Topic 606) ("ASU 2014-09"), which amends the existing accounting standards for revenue recognition. ASU 2014-09 is based on principles that govern the recognition of revenue at an amount an entity expects to be entitled when products are transferred to customers.

The original effective date for ASU 2014-09 would have required the Company to adopt beginning in its first quarter of 2018. In August 2015, the FASB issued ASU No. 2015-14, Revenue from Contracts with Customers (Topic 606) – Deferral of the Effective Date, which defers the effective date of ASU 2014-09 for one year and permits early adoption as early as the original effective date of ASU 2014-09. Accordingly, the Company may adopt the standard in either its first quarter of 2018 or 2019. The new revenue standard may be applied retrospectively to each prior period presented or retrospectively with the cumulative effect recognized as of the date of adoption. The Company is currently evaluating the timing of its adoption and the impact of adopting the new revenue standard on its consolidated financial statements.

Liquidity and Capital Resources

The following table presents selected financial information and statistics as of and for the years ended September 26, 2015, September 27, 2014 and September 28, 2013 (in millions):

	2015	2014	2013
Cash, cash equivalents and marketable securities	$ 205,666	$ 155,239	$ 146,761
Property, plant and equipment, net	$ 22,471	$ 20,624	$ 16,597
Commercial paper	$ 8,499	$ 6,308	$ 0
Total term debt	$ 55,963	$ 28,987	$ 16,960
Working capital	$ 8,768	$ 5,083	$ 29,628
Cash generated by operating activities	$ 81,266	$ 59,713	$ 53,666
Cash used in investing activities	$ (56,274)	$ (22,579)	$ (33,774)
Cash used in financing activities	$ (17,716)	$ (37,549)	$ (16,379)

The Company believes its existing balances of cash, cash equivalents and marketable securities will be sufficient to satisfy its working capital needs, capital asset purchases, outstanding commitments and other liquidity requirements associated with its existing operations over the next 12 months. The Company currently anticipates the cash used for future dividends, the share repurchase program and debt repayments will come from its current domestic cash, cash generated from on-going U.S. operating activities and from borrowings.

As of September 26, 2015 and September 27, 2014, the Company's cash, cash equivalents and marketable securities held by foreign subsidiaries were $186.9 billion and $137.1 billion, respectively, and are generally based in U.S. dollar-denominated holdings. Amounts held by foreign subsidiaries are generally subject to U.S. income taxation on repatriation to the U.S. The Company's marketable securities investment portfolio is invested primarily in highly-rated securities and its investment policy generally limits the amount of credit exposure to any one issuer. The policy requires investments generally to be investment grade with the objective of minimizing the potential risk of principal loss.

During 2015, cash generated from operating activities of $81.3 billion was a result of $53.4 billion of net income, non-cash adjustments to net income of $16.2 billion and an increase in the net change in operating assets and liabilities of $11.7 billion. Cash used in investing activities of $56.3 billion during 2015 consisted primarily of cash used for purchases of marketable securities, net of sales and maturities, of $44.4 billion and cash used to acquire property, plant and equipment of $11.2 billion. Cash used in financing activities of $17.7 billion during 2015 consisted primarily of cash used to repurchase common stock of $35.3 billion and cash used to pay dividends and dividend equivalents of $11.6 billion, partially offset by net proceeds from the issuance of term debt of $27.1 billion.

During 2014, cash generated from operating activities of $59.7 billion was a result of $39.5 billion of net income, non-cash adjustments to net income of $13.2 billion and an increase in net change in operating assets and liabilities of $7.0 billion. Cash used in investing activities of $22.6 billion during 2014 consisted primarily of cash used for purchases of marketable securities, net of sales and maturities, of $9.0 billion; cash used to acquire property, plant and equipment of $9.6 billion; and cash paid for business acquisitions, net of cash acquired, of $3.8 billion. Cash used in financing activities of $37.5 billion during 2014 consisted primarily of cash used to repurchase common stock of $45.0 billion and cash used to pay dividends and dividend equivalents of $11.1 billion, partially offset by net proceeds from the issuance of term debt and commercial paper of $12.0 billion and $6.3 billion, respectively.

Capital Assets

The Company's capital expenditures were $11.2 billion during 2015. The Company anticipates utilizing approximately $15.0 billion for capital expenditures during 2016, which includes product tooling and manufacturing process equipment; data centers; corporate facilities and infrastructure, including information systems hardware, software and enhancements; and retail store facilities.

Debt

In 2014, the Board of Directors authorized the Company to issue unsecured short-term promissory notes ("Commercial Paper") pursuant to a commercial paper program. The Company intends to use the net proceeds from the commercial paper program for general corporate purposes, including dividends and share repurchases. As of September 26, 2015, the Company had $8.5 billion of Commercial Paper outstanding, with a weighted-average interest rate of 0.14% and maturities generally less than nine months.

As of September 26, 2015, the Company has outstanding floating- and fixed-rate notes for an aggregate principal amount of $55.7 billion (collectively the "Notes"). The Company has entered, and in the future may enter, into interest rate swaps to manage interest rate risk on the Notes. In addition, the Company has entered, and in the future may enter, into currency swaps to manage foreign currency risk on the Notes. The future principal payments for the Company's Notes as of September 26, 2015 are as follows (in millions):

2016	$ 2,500
2017	3,500
2018	6,000
2019	3,775
2020	5,581
Thereafter	34,345
Total term debt	$ 55,701

Further information regarding the Company's debt issuances and related hedging activity can be found in Part II, Item 8 of this Form 10-K in the Notes to the Consolidated Financial Statements in Note 2, "Financial Instruments" and Note 6, "Debt."

Capital Return Program

In April 2015, the Company's Board of Directors increased the share repurchase program authorization from $90 billion to $140 billion of the Company's common stock, increasing the expected total size of the capital return program to $200 billion. The Company expects to execute the capital return program by the end of March 2017 by paying dividends and dividend equivalents, repurchasing shares and remitting withheld taxes related to net share settlement of restricted stock units. To assist in funding its capital return program, the Company expects to continue to access the debt markets, both domestically and internationally. As of September 26, 2015, $104 billion of the share repurchase program has been utilized. The Company's share repurchase program does not obligate it to acquire any specific number of shares. Under the program, shares may be repurchased in privately negotiated or open market transactions, including under plans complying with Rule 10b5-1 under the Securities Exchange Act of 1934, as amended.

In April 2015, the Company's Board of Directors raised the quarterly cash dividend by 11%. The Company plans to increase its dividend on an annual basis subject to declaration by the Board of Directors.

The following table presents the Company's dividends, dividend equivalents, share repurchases and net share settlement activity from the start of the capital return program in August 2012 through September 26, 2015 (in millions):

	Dividends and Dividend Equivalents Paid	Accelerated Share Repurchases	Open Market Share Repurchases	Taxes Related to Settlement of Equity Awards	Total
2015	$ 11,561	$ 6,000	$ 30,026	$ 1,499	$ 49,086
2014	11,126	21,000	24,000	1,158	57,284
2013	10,564	13,950	9,000	1,082	34,596
2012	2,488	0	0	56	2,544
Total	$ 35,739	$ 40,950	$ 63,026	$ 3,795	$ 143,510

Off-Balance Sheet Arrangements and Contractual Obligations

The Company has not entered into any transactions with unconsolidated entities whereby the Company has financial guarantees, subordinated retained interests, derivative instruments, or other contingent arrangements that expose the Company to material continuing risks, contingent liabilities, or any other obligation under a variable interest in an unconsolidated entity that provides financing, liquidity, market risk, or credit risk support to the Company, or engages in leasing, hedging, or R&D services with the Company.

The following table presents certain payments due by the Company under contractual obligations with minimum firm commitments as of September 26, 2015, and excludes amounts already recorded on the Consolidated Balance Sheet, except for term debt (in millions):

	Payments Due in Less Than 1 Year	Payments Due in 1-3 Years	Payments Due in 4-5 Years	Payments Due in More Than 5 Years	Total
Term debt	$ 2,500	$ 9,500	$ 9,356	$ 34,345	$ 55,701
Operating leases	772	1,518	1,389	2,592	6,271
Purchase commitments	29,464	0	0	0	29,464
Other obligations	4,553	1,898	53	757	7,261
Total	$ 37,289	$ 12,916	$ 10,798	$ 37,694	$ 98,697

Operating Leases

The Company's major facility leases are typically for terms not exceeding 10 years and generally contain multi-year renewal options. As of September 26, 2015, the Company had a total of 463 retail stores. Leases for retail space are for terms ranging from five to 20 years, the majority of which are for 10 years, and often contain multi-year renewal options. As of September 26, 2015, the Company's total future minimum lease payments under noncancelable operating leases were $6.3 billion, of which $3.6 billion related to leases for retail space.

Purchase Commitments

The Company utilizes several outsourcing partners to manufacture sub-assemblies for the Company's products and to perform final assembly and testing of finished products. These outsourcing partners acquire components and build product based on demand information supplied by the Company, which typically covers periods up to 150 days. The Company also obtains individual components for its products from a wide variety of individual suppliers. Consistent with industry practice, the Company acquires components through a combination of purchase orders, supplier contracts, and open orders based on projected demand information. Where appropriate, the purchases are applied to inventory component prepayments that are outstanding with the respective supplier. As of September 26, 2015, the Company had outstanding off-balance sheet third-party manufacturing commitments and component purchase commitments of $29.5 billion.

Other Obligations

The Company's other off-balance sheet obligations were comprised of commitments to acquire capital assets, including product tooling and manufacturing process equipment, and commitments related to inventory prepayments, advertising, licensing, R&D, internet and telecommunications services, energy and other obligations.

The Company's other non-current liabilities in the Consolidated Balance Sheets consist primarily of deferred tax liabilities, gross unrecognized tax benefits and the related gross interest and penalties. As of September 26, 2015, the Company had non-current deferred tax liabilities of $24.1 billion. Additionally, as of September 26, 2015, the Company had gross unrecognized tax benefits of $6.9 billion and an additional $1.3 billion for gross interest and penalties classified as non-current liabilities. At this time, the Company is unable to make a reasonably reliable estimate of the timing of payments in individual years in connection with these tax liabilities; therefore, such amounts are not included in the above contractual obligation table.

Indemnification

The Company generally does not indemnify end-users of its operating system and application software against legal claims that the software infringes third-party intellectual property rights. Other agreements entered into by the Company sometimes include indemnification provisions under which the Company could be subject to costs and/or damages in the event of an infringement claim against the Company or an indemnified third-party. In the opinion of management, there was not at least a reasonable possibility the Company may have incurred a material loss with respect to indemnification of end-users of its operating system or application software for infringement of third-party intellectual property rights. The Company did not record a liability for infringement costs related to indemnification as of September 26, 2015 or September 27, 2014.

In September 2015, the Company introduced the iPhone Upgrade Program, which is available to customers who purchase an iPhone 6s and 6s Plus in one of its U.S. physical retail stores and activate the purchased iPhone with one of the four national carriers. The iPhone Upgrade Program provides customers the right to trade in that iPhone for a new iPhone, provided certain conditions are met. One of the conditions of this program requires the customer to finance the initial purchase price of the iPhone with a third-party lender. Upon exercise of the trade-in right and purchase of a new iPhone, the Company satisfies the customer's outstanding balance due to the third-party lender on the original device. The Company accounts for the trade-in right as a guarantee liability and recognizes arrangement revenue net of the fair value of such right with subsequent changes to the guarantee liability recognized within revenue.

The Company has entered into indemnification agreements with its directors and executive officers. Under these agreements, the Company has agreed to indemnify such individuals to the fullest extent permitted by law against liabilities that arise by reason of their status as directors or officers and to advance expenses incurred by such individuals in connection with related legal proceedings. It is not possible to determine the maximum potential amount of payments the Company could be required to make under these agreements due to the limited history of prior indemnification claims and the unique facts and circumstances involved in each claim. However, the Company maintains directors and officers liability insurance coverage to reduce its exposure to such obligations.

Critical Accounting Policies and Estimates

The preparation of financial statements and related disclosures in conformity with U.S. generally accepted accounting principles ("GAAP") and the Company's discussion and analysis of its financial condition and operating results require the Company's management to make judgments, assumptions and estimates that affect the amounts reported in its consolidated financial statements and accompanying notes. Note 1, "Summary of Significant Accounting Policies," of the Notes to Consolidated Financial Statements in Part II, Item 8 of this Form 10-K describes the significant accounting policies and methods used in the preparation of the Company's consolidated financial statements. Management bases its estimates on historical experience and on various other assumptions it believes to be reasonable under the circumstances, the results of which form the basis for making judgments about the carrying values of assets and liabilities. Actual results may differ from these estimates, and such differences may be material.

Management believes the Company's critical accounting policies and estimates are those related to revenue recognition, valuation and impairment of marketable securities, inventory valuation and valuation of manufacturing-related assets and estimated purchase commitment cancellation fees, warranty costs, income taxes, and legal and other contingencies. Management considers these policies critical because they are both important to the portrayal of the Company's financial condition and operating results, and they require management to make judgments and estimates about inherently uncertain matters. The Company's senior management has reviewed these critical accounting policies and related disclosures with the Audit and Finance Committee of the Company's Board of Directors.

Revenue Recognition

Net sales consist primarily of revenue from the sale of hardware, software, digital content and applications, accessories, and service and support contracts. The Company recognizes revenue when persuasive evidence of an arrangement exists, delivery has occurred, the sales price is fixed or determinable and collection is probable. Product is considered delivered to the customer once it has been shipped and title, risk of loss and rewards of ownership have been transferred. For most of the Company's product sales, these criteria are met at the time the product is shipped. For online sales to individuals, for some sales to education customers in the U.S., and for certain other sales, the Company defers revenue until the customer receives the product because the Company retains a portion of the risk of loss on these sales during transit. For payment terms in excess of the Company's standard payment terms, revenue is recognized as payments become due unless the Company has positive evidence that the sales price is fixed or determinable, such as a successful history of collection, without concession, on comparable arrangements. The Company recognizes revenue from the sale of hardware products, software bundled with hardware that is essential to the functionality of the hardware and third-party digital content sold on the iTunes Store in accordance with general revenue recognition accounting guidance. The Company recognizes revenue in accordance with industry-specific software accounting guidance for the following types of sales transactions: (i) standalone sales of software products, (ii) sales of software upgrades and (iii) sales of software bundled with hardware not essential to the functionality of the hardware.

For multi-element arrangements that include hardware products containing software essential to the hardware product's functionality, undelivered software elements that relate to the hardware product's essential software and/or undelivered non-software services, the Company allocates revenue to all deliverables based on their relative selling prices. In such circumstances, the Company uses a hierarchy to determine the selling price to be used for allocating revenue to deliverables: (i) vendor-specific objective evidence of fair value ("VSOE"), (ii) third-party evidence of selling price ("TPE") and (iii) best estimate of selling price ("ESP"). VSOE generally exists only when the Company sells the deliverable separately and is the price actually charged by the Company for that deliverable. ESPs reflect the Company's best estimates of what the selling prices of elements would be if they were sold regularly on a stand-alone basis.

For sales of qualifying versions of iOS devices, Mac, Apple Watch and Apple TV, the Company has indicated it may from time to time provide future unspecified software upgrades to the device's essential software and/or non-software services free of charge. Because the Company has neither VSOE nor TPE for the unspecified software upgrade rights or the non-software services, revenue is allocated to these rights and services based on the Company's ESPs. Revenue allocated to the unspecified software upgrade rights and non-software services based on the Company's ESPs is deferred and recognized on a straight-line basis over the estimated period the software upgrades and non-software services are expected to be provided.

The Company's process for determining ESPs involves management's judgment and considers multiple factors that may vary over time depending upon the unique facts and circumstances related to each deliverable. Should future facts and circumstances change, the Company's ESPs and the future rate of related amortization for unspecified software upgrades and non-software services related to future sales of these devices could change. Factors subject to change include the unspecified software upgrade rights and non-software services offered, the estimated value of unspecified software upgrade rights and non-software services and the estimated period unspecified software upgrades and non-software services are expected to be provided.

The Company records reductions to revenue for estimated commitments related to price protection and other customer incentive programs. For transactions involving price protection, the Company recognizes revenue net of the estimated amount to be refunded, provided the refund amount can be reasonably and reliably estimated and the other conditions for revenue recognition have been met. The Company's policy requires that, if refunds cannot be reliably estimated, revenue is not recognized until reliable estimates can be made or the price protection lapses. For the Company's other customer incentive programs, the estimated cost is recognized at the later of the date at which the Company has sold the product or the date at which the program is offered. The Company also records reductions to revenue for expected future product returns based on the Company's historical experience. Future market conditions and product transitions may require the Company to increase customer incentive programs that could result in reductions to future revenue. Additionally, certain customer incentive programs require management to estimate the number of customers who will actually redeem the incentive. Management's estimates are based on historical experience and the specific terms and conditions of particular incentive programs. If a greater than estimated proportion of customers redeems such incentives, the Company would be required to record additional reductions to revenue, which would have an adverse impact on the Company's operating results.

Valuation and Impairment of Marketable Securities

The Company's investments in available-for-sale securities are reported at fair value. Unrealized gains and losses related to changes in the fair value of securities are recognized in accumulated other comprehensive income, net of tax, in the Company's Consolidated Balance Sheets. Changes in the fair value of available-for-sale securities impact the Company's net income only when such securities are sold or an other-than-temporary impairment is recognized. Realized gains and losses on the sale of securities are determined by specific identification of each security's cost basis. The Company regularly reviews its investment portfolio to determine if any security is other-than-temporarily impaired, which would require the Company to record an impairment charge in the period any such determination is made. In making this judgment, the Company evaluates, among other things, the duration and extent to which the fair value of a security is less than its cost; the financial condition of the issuer and any changes thereto; and the Company's intent to sell, or whether it will more likely than not be required to sell, the security before recovery of its amortized cost basis. The Company's assessment on whether a security is other-than-temporarily impaired could change in the future due to new developments or changes in assumptions related to any particular security, which would have an adverse impact on the Company's operating results.

Inventory Valuation and Valuation of Manufacturing-Related Assets and Estimated Purchase Commitment Cancellation Fees

The Company must purchase components and build inventory in advance of product shipments and has invested in manufacturing-related assets, including capital assets held at its suppliers' facilities. In addition, the Company has made prepayments to certain of its suppliers associated with long-term supply agreements to secure supply of inventory components. The Company records a write-down for inventories of components and products, including third-party products held for resale, which have become obsolete or are in excess of anticipated demand or net realizable value. The Company performs a detailed review of inventory that considers multiple factors including demand forecasts, product life cycle status, product development plans, current sales levels and component cost trends. The Company also reviews its manufacturing-related capital assets and inventory prepayments for impairment whenever events or circumstances indicate the carrying amount of such assets may not be recoverable. If the Company determines that an asset is not recoverable, it records an impairment loss equal to the amount by which the carrying value of such an asset exceeds its fair value.

The industries in which the Company competes are subject to a rapid and unpredictable pace of product and component obsolescence and demand changes. In certain circumstances the Company may be required to record additional write-downs of inventory and/or manufacturing-related assets. These circumstances include future demand or market conditions for the Company's products being less favorable than forecasted, unforeseen technological changes or changes to the Company's product development plans that negatively impact the utility of any of these assets, or significant deterioration in the financial condition of one or more of the Company's suppliers that hold any of the Company's manufacturing-related assets or to whom the Company has made an inventory prepayment. Such write-downs would adversely affect the Company's financial condition and operating results in the period when the write-downs were recorded.

The Company accrues for estimated cancellation fees related to inventory orders that have been cancelled or are expected to be cancelled. Consistent with industry practice, the Company acquires components through a combination of purchase orders, supplier contracts, and open orders in each case based on projected demand. Where appropriate, the purchases are applied to inventory component prepayments that are outstanding with the respective supplier. Purchase commitments typically cover the Company's forecasted component and manufacturing requirements for periods up to 150 days. If there is an abrupt and substantial decline in demand for one or more of the Company's products, a change in the Company's product development plans, or an unanticipated change in technological requirements for any of the Company's products, the Company may be required to record additional accruals for cancellation fees that would adversely affect its results of operations in the period when the cancellation fees are identified and recorded.

Warranty Costs

The Company accrues for the estimated cost of warranties at the time the related revenue is recognized based on historical and projected warranty claim rates, historical and projected cost-per-claim and knowledge of specific product failures that are outside of the Company's typical experience. The Company regularly reviews these estimates to assess the adequacy of its recorded warranty liabilities or the current installed base of products subject to warranty protection and adjusts the amounts as necessary. If actual product failure rates or repair costs differ from estimates, revisions to the estimated warranty liabilities would be required and could materially affect the Company's financial condition and operating results.

Income Taxes

The Company records a tax provision for the anticipated tax consequences of its reported operating results. The provision for income taxes is computed using the asset and liability method, under which deferred tax assets and liabilities are recognized for the expected future tax consequences of temporary differences between the financial reporting and tax bases of assets and liabilities, and for operating losses and tax credit carryforwards. Deferred tax assets and liabilities are measured using the currently enacted tax rates that apply to taxable income in effect for the years in which those tax assets and liabilities are expected to be realized or settled. The Company records a valuation allowance to reduce deferred tax assets to the amount that is believed more likely than not to be realized.

The Company recognizes tax benefits from uncertain tax positions only if it is more likely than not that the tax position will be sustained on examination by the taxing authorities, based on the technical merits of the position. The tax benefits recognized in the financial statements from such positions are then measured based on the largest benefit that has a greater than 50% likelihood of being realized upon ultimate settlement.

Management believes it is more likely than not that forecasted income, including income that may be generated as a result of certain tax planning strategies, together with future reversals of existing taxable temporary differences, will be sufficient to fully recover the deferred tax assets. In the event that the Company determines all or part of the net deferred tax assets are not realizable in the future, the Company will record an adjustment to the valuation allowance that would be charged to earnings in the period such determination is made. In addition, the calculation of tax liabilities involves significant judgment in estimating the impact of uncertainties in the application of GAAP and complex tax laws. Resolution of these uncertainties in a manner inconsistent with management's expectations could have a material impact on the Company's financial condition and operating results.

Legal and Other Contingencies

As discussed in Part I, Item 3 of this Form 10-K under the heading "Legal Proceedings" and in Part II, Item 8 of this Form 10-K in the Notes to Consolidated Financial Statements in Note 10, "Commitments and Contingencies," the Company is subject to various legal proceedings and claims that arise in the ordinary course of business. The Company records a liability when it is probable that a loss has been incurred and the amount is reasonably estimable. There is significant judgment required in both the probability determination and as to whether an exposure can be reasonably estimated. In the opinion of management, there was not at least a reasonable possibility the Company may have incurred a material loss, or a material loss in excess of a recorded accrual, with respect to loss contingencies for asserted legal and other claims. However, the outcome of legal proceedings and claims brought against the Company is subject to significant uncertainty. Therefore, although management considers the likelihood of such an outcome to be remote, if one or more of these legal matters were resolved against the Company in a reporting period for amounts in excess of management's expectations, the Company's consolidated financial statements for that reporting period could be materially adversely affected.

Item 7A. Quantitative and Qualitative Disclosures About Market Risk

Interest Rate and Foreign Currency Risk Management

The Company regularly reviews its foreign exchange forward and option positions and interest rate swaps, both on a stand-alone basis and in conjunction with its underlying foreign currency and interest rate related exposures. Given the effective horizons of the Company's risk management activities and the anticipatory nature of the exposures, there can be no assurance these positions will offset more than a portion of the financial impact resulting from movements in either foreign exchange or interest rates. Further, the recognition of the gains and losses related to these instruments may not coincide with the timing of gains and losses related to the underlying economic exposures and, therefore, may adversely affect the Company's financial condition and operating results.

Interest Rate Risk

The Company's exposure to changes in interest rates relates primarily to the Company's investment portfolio and outstanding debt. While the Company is exposed to global interest rate fluctuations, the Company's interest income and expense are most sensitive to fluctuations in U.S. interest rates. Changes in U.S. interest rates affect the interest earned on the Company's cash, cash equivalents and marketable securities and the fair value of those securities, as well as costs associated with hedging and interest paid on the Company's debt.

The Company's investment policy and strategy are focused on preservation of capital and supporting the Company's liquidity requirements. The Company uses a combination of internal and external management to execute its investment strategy and achieve its investment objectives. The Company typically invests in highly-rated securities, and its investment policy generally limits the amount of credit exposure to any one issuer. The policy requires investments generally to be investment grade, with the primary objective of minimizing the potential risk of principal loss. To provide a meaningful assessment of the interest rate risk associated with the Company's investment portfolio, the Company performed a sensitivity analysis to determine the impact a change in interest rates would have on the value of the investment portfolio assuming a 100 basis point parallel shift in the yield curve. Based on investment positions as of September 26, 2015 and September 27, 2014, a hypothetical 100 basis point increase in interest rates across all maturities would result in a $4.3 billion and $3.4 billion incremental decline in the fair market value of the portfolio, respectively. Such losses would only be realized if the Company sold the investments prior to maturity.

As of September 26, 2015 and September 27, 2014, the Company had outstanding floating- and fixed-rate notes with varying maturities for an aggregate carrying amount of $56.0 billion and $29.0 billion, respectively. The Company has entered, and may enter in the future, into interest rate swaps to manage interest rate risk on its outstanding term debt. Interest rate swaps allow the Company to effectively convert fixed-rate payments into floating-rate payments or floating-rate payments into fixed-rate payments. Gains and losses on these instruments are generally offset by the corresponding losses and gains on the related hedging instrument. A 100 basis point increase in market interest rates would cause interest expense on the Company's debt as of September 26, 2015 and September 27, 2014 to increase by $200 million and $110 million on an annualized basis, respectively.

Further details regarding the Company's debt is provided in Part II, Item 8 of this Form 10-K in the Notes to Consolidated Financial Statements in Note 6, "Debt."

Foreign Currency Risk

In general, the Company is a net receiver of currencies other than the U.S. dollar. Accordingly, changes in exchange rates, and in particular a strengthening of the U.S. dollar, will negatively affect the Company's net sales and gross margins as expressed in U.S. dollars. There is a risk that the Company will have to adjust local currency product pricing due to competitive pressures when there have been significant volatility in foreign currency exchange rates.

The Company may enter into foreign currency forward and option contracts with financial institutions to protect against foreign exchange risks associated with certain existing assets and liabilities, certain firmly committed transactions, forecasted future cash flows and net investments in foreign subsidiaries. In addition, the Company has entered, and may enter in the future, into non-designated foreign currency contracts to partially offset the foreign currency exchange gains and losses on its foreign-denominated debt issuances. The Company's practice is to hedge a portion of its material foreign exchange exposures, typically for up to 12 months. However, the Company may choose not to hedge certain foreign exchange exposures for a variety of reasons, including but not limited to accounting considerations and the prohibitive economic cost of hedging particular exposures.

To provide a meaningful assessment of the foreign currency risk associated with certain of the Company's foreign currency derivative positions, the Company performed a sensitivity analysis using a value-at-risk ("VAR") model to assess the potential impact of fluctuations in exchange rates. The VAR model consisted of using a Monte Carlo simulation to generate thousands of random market price paths assuming normal market conditions. The VAR is the maximum expected loss in fair value, for a given confidence interval, to the Company's foreign currency derivative positions due to adverse movements in rates. The VAR model is not intended to represent actual losses but is used as a risk estimation and management tool. The model assumes normal market conditions. Forecasted transactions, firm commitments and assets and liabilities denominated in foreign currencies were excluded from the model. Based on the results of the model, the Company estimates with 95% confidence a maximum one-day loss in fair value of $342 million as of September 26, 2015 compared to a maximum one-day loss in fair value of $240 million as of September 27, 2014. Because the Company uses foreign currency instruments for hedging purposes, the loss in fair value incurred on those instruments are generally offset by increases in the fair value of the underlying exposures.

Actual future gains and losses associated with the Company's investment portfolio and derivative positions may differ materially from the sensitivity analyses performed as of September 26, 2015 due to the inherent limitations associated with predicting the timing and amount of changes in interest rates, foreign currency exchanges rates and the Company's actual exposures and positions.

Item 8. Financial Statements and Supplementary Data

All financial statement schedules have been omitted, since the required information is not applicable or is not present in amounts sufficient to require submission of the schedule, or because the information required is included in the consolidated financial statements and notes thereto.

CONSOLIDATED STATEMENTS OF OPERATIONS

(In millions, except number of shares which are reflected in thousands and per share amounts)

	Years ended		
	September 26, 2015	September 27, 2014	September 28, 2013
Net sales	$ 233,715	$ 182,795	$ 170,910
Cost of sales	140,089	112,258	106,606
Gross margin	93,626	70,537	64,304
Operating expenses:			
Research and development	8,067	6,041	4,475
Selling, general and administrative	14,329	11,993	10,830
Total operating expenses	22,396	18,034	15,305
Operating income	71,230	52,503	48,999
Other income/(expense), net	1,285	980	1,156
Income before provision for income taxes	72,515	53,483	50,155
Provision for income taxes	19,121	13,973	13,118
Net income	$ 53,394	$ 39,510	$ 37,037
Earnings per share:			
Basic	$ 9.28	$ 6.49	$ 5.72
Diluted	$ 9.22	$ 6.45	$ 5.68
Shares used in computing earnings per share:			
Basic	5,753,421	6,085,572	6,477,320
Diluted	5,793,069	6,122,663	6,521,634
Cash dividends declared per share	$ 1.98	$ 1.82	$ 1.64

See accompanying Notes to Consolidated Financial Statements.

CONSOLIDATED STATEMENTS OF COMPREHENSIVE INCOME

(In millions)

	Years ended		
	September 26, 2015	September 27, 2014	September 28, 2013
Net income	$ 53,394	$ 39,510	$ 37,037
Other comprehensive income/(loss):			
Change in foreign currency translation, net of tax effects of $201, $50 and $35, respectively	(411)	(137)	(112)
Change in unrealized gains/losses on derivative instruments:			
Change in fair value of derivatives, net of tax benefit/(expense) of $(441), $(297) and $(351), respectively	2,905	1,390	522
Adjustment for net (gains)/losses realized and included in net income, net of tax expense/(benefit) of $630, $(36) and $255, respectively	(3,497)	149	(458)
Total change in unrealized gains/losses on derivative instruments, net of tax	(592)	1,539	64
Change in unrealized gains/losses on marketable securities:			
Change in fair value of marketable securities, net of tax benefit/(expense) of $264, $(153) and $458, respectively	(483)	285	(791)
Adjustment for net (gains)/losses realized and included in net income, net of tax expense/(benefit) of $(32), $71 and $82, respectively	59	(134)	(131)
Total change in unrealized gains/losses on marketable securities, net of tax	(424)	151	(922)
Total other comprehensive income/(loss)	(1,427)	1,553	(970)
Total comprehensive income	$ 51,967	$ 41,063	$ 36,067

See accompanying Notes to Consolidated Financial Statements.

CONSOLIDATED BALANCE SHEETS

(In millions, except number of shares which are reflected in thousands and par value)

	September 26, 2015	September 27, 2014
ASSETS:		
Current assets:		
Cash and cash equivalents	$ 21,120	$ 13,844
Short-term marketable securities	20,481	11,233
Accounts receivable, less allowances of $82 and $86, respectively	16,849	17,460
Inventories	2,349	2,111
Deferred tax assets	5,546	4,318
Vendor non-trade receivables	13,494	9,759
Other current assets	9,539	9,806
Total current assets	89,378	68,531
Long-term marketable securities	164,065	130,162
Property, plant and equipment, net	22,471	20,624
Goodwill	5,116	4,616
Acquired intangible assets, net	3,893	4,142
Other assets	5,556	3,764
Total assets	$ 290,479	$ 231,839
LIABILITIES AND SHAREHOLDERS' EQUITY:		
Current liabilities:		
Accounts payable	$ 35,490	$ 30,196
Accrued expenses	25,181	18,453
Deferred revenue	8,940	8,491
Commercial paper	8,499	6,308
Current portion of long-term debt	2,500	0
Total current liabilities	80,610	63,448
Deferred revenue, non-current	3,624	3,031
Long-term debt	53,463	28,987
Other non-current liabilities	33,427	24,826
Total liabilities	171,124	120,292
Commitments and contingencies		
Shareholders' equity:		
Common stock and additional paid-in capital, $0.00001 par value: 12,600,000 shares authorized; 5,578,753 and 5,866,161 shares issued and outstanding, respectively	27,416	23,313
Retained earnings	92,284	87,152
Accumulated other comprehensive income	(345)	1,082
Total shareholders' equity	119,355	111,547
Total liabilities and shareholders' equity	$ 290,479	$ 231,839

See accompanying Notes to Consolidated Financial Statements.

CONSOLIDATED STATEMENTS OF SHAREHOLDERS' EQUITY

(In millions, except number of shares which are reflected in thousands)

	Common Stock and Additional Paid-In Capital		Retained Earnings	Accumulated Other Comprehensive Income/(Loss)	Total Shareholders' Equity
	Shares	Amount			
Balances as of September 29, 2012	6,574,458	$ 16,422	$ 101,289	$ 499	$ 118,210
Net income	0	0	37,037	0	37,037
Other comprehensive income/(loss)	0	0	0	(970)	(970)
Dividends and dividend equivalents declared	0	0	(10,676)	0	(10,676)
Repurchase of common stock	(328,837)	0	(22,950)	0	(22,950)
Share-based compensation	0	2,253	0	0	2,253
Common stock issued, net of shares withheld for employee taxes	48,873	(143)	(444)	0	(587)
Tax benefit from equity awards, including transfer pricing adjustments	0	1,232	0	0	1,232
Balances as of September 28, 2013	6,294,494	19,764	104,256	(471)	123,549
Net income	0	0	39,510	0	39,510
Other comprehensive income/(loss)	0	0	0	1,553	1,553
Dividends and dividend equivalents declared	0	0	(11,215)	0	(11,215)
Repurchase of common stock	(488,677)	0	(45,000)	0	(45,000)
Share-based compensation	0	2,863	0	0	2,863
Common stock issued, net of shares withheld for employee taxes	60,344	(49)	(399)	0	(448)
Tax benefit from equity awards, including transfer pricing adjustments	0	735	0	0	735
Balances as of September 27, 2014	5,866,161	23,313	87,152	1,082	111,547
Net income	0	0	53,394	0	53,394
Other comprehensive income/(loss)	0	0	0	(1,427)	(1,427)
Dividends and dividend equivalents declared	0	0	(11,627)	0	(11,627)
Repurchase of common stock	(325,032)	0	(36,026)	0	(36,026)
Share-based compensation	0	3,586	0	0	3,586
Common stock issued, net of shares withheld for employee taxes	37,624	(231)	(609)	0	(840)
Tax benefit from equity awards, including transfer pricing adjustments	0	748	0	0	748
Balances as of September 26, 2015	5,578,753	$ 27,416	$ 92,284	$ (345)	$ 119,355

See accompanying Notes to Consolidated Financial Statements.

CONSOLIDATED STATEMENTS OF CASH FLOWS

(In millions)

	Years ended		
	September 26, 2015	September 27, 2014	September 28, 2013
Cash and cash equivalents, beginning of the year	$ 13,844	$ 14,259	$ 10,746
Operating activities:			
Net income	53,394	39,510	37,037
Adjustments to reconcile net income to cash generated by operating activities:			
Depreciation and amortization	11,257	7,946	6,757
Share-based compensation expense	3,586	2,863	2,253
Deferred income tax expense	1,382	2,347	1,141
Changes in operating assets and liabilities:			
Accounts receivable, net	611	(4,232)	(2,172)
Inventories	(238)	(76)	(973)
Vendor non-trade receivables	(3,735)	(2,220)	223
Other current and non-current assets	(179)	167	1,080
Accounts payable	5,400	5,938	2,340
Deferred revenue	1,042	1,460	1,459
Other current and non-current liabilities	8,746	6,010	4,521
Cash generated by operating activities	81,266	59,713	53,666
Investing activities:			
Purchases of marketable securities	(166,402)	(217,128)	(148,489)
Proceeds from maturities of marketable securities	14,538	18,810	20,317
Proceeds from sales of marketable securities	107,447	189,301	104,130
Payments made in connection with business acquisitions, net	(343)	(3,765)	(496)
Payments for acquisition of property, plant and equipment	(11,247)	(9,571)	(8,165)
Payments for acquisition of intangible assets	(241)	(242)	(911)
Other	(26)	16	(160)
Cash used in investing activities	(56,274)	(22,579)	(33,774)
Financing activities:			
Proceeds from issuance of common stock	543	730	530
Excess tax benefits from equity awards	749	739	701
Taxes paid related to net share settlement of equity awards	(1,499)	(1,158)	(1,082)
Dividends and dividend equivalents paid	(11,561)	(11,126)	(10,564)
Repurchase of common stock	(35,253)	(45,000)	(22,860)
Proceeds from issuance of term debt, net	27,114	11,960	16,896
Change in commercial paper, net	2,191	6,306	0
Cash used in financing activities	(17,716)	(37,549)	(16,379)
Increase/(decrease) in cash and cash equivalents	7,276	(415)	3,513
Cash and cash equivalents, end of the year	$ 21,120	$ 13,844	$ 14,259
Supplemental cash flow disclosure:			
Cash paid for income taxes, net	$ 13,252	$ 10,026	$ 9,128
Cash paid for interest	$ 514	$ 339	$ 0

See accompanying Notes to Consolidated Financial Statements.

Note 1 – Summary of Significant Accounting Policies

Apple Inc. and its wholly-owned subsidiaries (collectively "Apple" or the "Company") designs, manufactures and markets mobile communication and media devices, personal computers and portable digital music players, and sells a variety of related software, services, accessories, networking solutions and third-party digital content and applications. The Company sells its products worldwide through its retail stores, online stores and direct sales force, as well as through third-party cellular network carriers, wholesalers, retailers and value-added resellers. In addition, the Company sells a variety of third-party Apple-compatible products, including application software and various accessories through its online and retail stores. The Company sells to consumers, small and mid-sized businesses and education, enterprise and government customers.

Basis of Presentation and Preparation

The accompanying consolidated financial statements include the accounts of the Company. Intercompany accounts and transactions have been eliminated. In the opinion of the Company's management, the consolidated financial statements reflect all adjustments, which are normal and recurring in nature, necessary for fair financial statement presentation. The preparation of these consolidated financial statements in conformity with U.S. generally accepted accounting principles ("GAAP") requires management to make estimates and assumptions that affect the amounts reported in these consolidated financial statements and accompanying notes. Actual results could differ materially from those estimates.

The Company's fiscal year is the 52 or 53-week period that ends on the last Saturday of September. The Company's fiscal years 2015, 2014 and 2013 ended on September 26, 2015, September 27, 2014 and September 28, 2013, respectively. An additional week is included in the first fiscal quarter approximately every six years to realign fiscal quarters with calendar quarters. Fiscal years 2015, 2014 and 2013 each spanned 52 weeks. Unless otherwise stated, references to particular years, quarters, months and periods refer to the Company's fiscal years ended in September and the associated quarters, months and periods of those fiscal years.

Revenue Recognition

Net sales consist primarily of revenue from the sale of hardware, software, digital content and applications, accessories, and service and support contracts. The Company recognizes revenue when persuasive evidence of an arrangement exists, delivery has occurred, the sales price is fixed or determinable and collection is probable. Product is considered delivered to the customer once it has been shipped and title, risk of loss and rewards of ownership have been transferred. For most of the Company's product sales, these criteria are met at the time the product is shipped. For online sales to individuals, for some sales to education customers in the U.S., and for certain other sales, the Company defers revenue until the customer receives the product because the Company retains a portion of the risk of loss on these sales during transit. For payment terms in excess of the Company's standard payment terms, revenue is recognized as payments become due unless the Company has positive evidence that the sales price is fixed or determinable, such as a successful history of collection, without concession, on comparable arrangements. The Company recognizes revenue from the sale of hardware products, software bundled with hardware that is essential to the functionality of the hardware and third-party digital content sold on the iTunes Store in accordance with general revenue recognition accounting guidance. The Company recognizes revenue in accordance with industry specific software accounting guidance for the following types of sales transactions: (i) standalone sales of software products, (ii) sales of software upgrades and (iii) sales of software bundled with hardware not essential to the functionality of the hardware.

For the sale of most third-party products, the Company recognizes revenue based on the gross amount billed to customers because the Company establishes its own pricing for such products, retains related inventory risk for physical products, is the primary obligor to the customer and assumes the credit risk for amounts billed to its customers. For third-party applications sold through the App Store and Mac App Store and certain digital content sold through the iTunes Store, the Company does not determine the selling price of the products and is not the primary obligor to the customer. Therefore, the Company accounts for such sales on a net basis by recognizing in net sales only the commission it retains from each sale. The portion of the gross amount billed to customers that is remitted by the Company to third-party app developers and certain digital content owners is not reflected in the Company's Consolidated Statements of Operations.

The Company records deferred revenue when it receives payments in advance of the delivery of products or the performance of services. This includes amounts that have been deferred for unspecified and specified software upgrade rights and non-software services that are attached to hardware and software products. The Company sells gift cards redeemable at its retail and online stores, and also sells gift cards redeemable on iTunes Store, App Store, Mac App Store and iBooks Store for the purchase of digital content and software. The Company records deferred revenue upon the sale of the card, which is relieved upon redemption of the card by the customer. Revenue from AppleCare service and support contracts is deferred and recognized over the service coverage periods. AppleCare service and support contracts typically include extended phone support, repair services, web-based support resources and diagnostic tools offered under the Company's standard limited warranty.

The Company records reductions to revenue for estimated commitments related to price protection and other customer incentive programs. For transactions involving price protection, the Company recognizes revenue net of the estimated amount to be refunded. For the Company's other customer incentive programs, the estimated cost of these programs is recognized at the later of the date at which the Company has sold the product or the date at which the program is offered. The Company also records reductions to revenue for expected future product returns based on the Company's historical experience. Revenue is recorded net of taxes collected from customers that are remitted to governmental authorities, with the collected taxes recorded as current liabilities until remitted to the relevant government authority.

Revenue Recognition for Arrangements with Multiple Deliverables

For multi-element arrangements that include hardware products containing software essential to the hardware product's functionality, undelivered software elements that relate to the hardware product's essential software, and undelivered non-software services, the Company allocates revenue to all deliverables based on their relative selling prices. In such circumstances, the Company uses a hierarchy to determine the selling price to be used for allocating revenue to deliverables: (i) vendor-specific objective evidence of fair value ("VSOE"), (ii) third-party evidence of selling price ("TPE") and (iii) best estimate of selling price ("ESP"). VSOE generally exists only when the Company sells the deliverable separately and is the price actually charged by the Company for that deliverable. ESPs reflect the Company's best estimates of what the selling prices of elements would be if they were sold regularly on a stand-alone basis. For multi-element arrangements accounted for in accordance with industry specific software accounting guidance, the Company allocates revenue to all deliverables based on the VSOE of each element, and if VSOE does not exist revenue is recognized when elements lacking VSOE are delivered.

For sales of qualifying versions of iPhone, iPad and iPod touch ("iOS devices"), Mac, Apple Watch and Apple TV, the Company has indicated it may from time to time provide future unspecified software upgrades to the device's essential software and/or non-software services free of charge. The Company has identified up to three deliverables regularly included in arrangements involving the sale of these devices. The first deliverable, which represents the substantial portion of the allocated sales price, is the hardware and software essential to the functionality of the hardware device delivered at the time of sale. The second deliverable is the embedded right included with qualifying devices to receive on a when-and-if-available basis, future unspecified software upgrades relating to the product's essential software. The third deliverable is the non-software services to be provided to qualifying devices. The Company allocates revenue between these deliverables using the relative selling price method. Because the Company has neither VSOE nor TPE for these deliverables, the allocation of revenue is based on the Company's ESPs. Revenue allocated to the delivered hardware and the related essential software is recognized at the time of sale provided the other conditions for revenue recognition have been met. Revenue allocated to the embedded unspecified software upgrade rights and the non-software services is deferred and recognized on a straight-line basis over the estimated period the software upgrades and non-software services are expected to be provided. Cost of sales related to delivered hardware and related essential software, including estimated warranty costs, are recognized at the time of sale. Costs incurred to provide non-software services are recognized as cost of sales as incurred, and engineering and sales and marketing costs are recognized as operating expenses as incurred.

The Company's process for determining its ESP for deliverables without VSOE or TPE considers multiple factors that may vary depending upon the unique facts and circumstances related to each deliverable including, where applicable, prices charged by the Company and market trends in the pricing for similar offerings, product specific business objectives, length of time a particular version of a device has been available, estimated cost to provide the non-software services and the relative ESP of the upgrade rights and non-software services as compared to the total selling price of the product.

Beginning in September 2015, the Company reduced the combined ESPs for iOS devices and Mac between $5 and $10 to reflect the increase in competitive offers for similar products at little to no cost for users, which reduces the amount the Company could reasonably charge for these deliverables on a standalone basis.

Shipping Costs

Amounts billed to customers related to shipping and handling are classified as revenue, and the Company's shipping and handling costs are classified as cost of sales.

Warranty Costs

The Company generally provides for the estimated cost of hardware and software warranties at the time the related revenue is recognized. The Company assesses the adequacy of its accrued warranty liabilities and adjusts the amounts as necessary based on actual experience and changes in future estimates.

Software Development Costs

Research and development ("R&D") costs are expensed as incurred. Development costs of computer software to be sold, leased, or otherwise marketed are subject to capitalization beginning when a product's technological feasibility has been established and ending when a product is available for general release to customers. In most instances, the Company's products are released soon after technological feasibility has been established and as a result software development costs were expensed as incurred.

Advertising Costs

Advertising costs are expensed as incurred and included in selling, general and administrative expenses. Advertising expense was $1.8 billion, $1.2 billion and $1.1 billion for 2015, 2014 and 2013, respectively.

Share-based Compensation

The Company recognizes expense related to share-based payment transactions in which it receives employee services in exchange for (a) equity instruments of the Company or (b) liabilities that are based on the fair value of the Company's equity instruments or that may be settled by the issuance of such equity instruments. Share-based compensation cost for restricted stock and restricted stock units ("RSUs") is measured based on the closing fair market value of the Company's common stock on the date of grant. The Company recognizes share-based compensation cost over the award's requisite service period on a straight-line basis for time-based RSUs and on a graded basis for RSUs that are contingent on the achievement of performance conditions. The Company recognizes a benefit from share-based compensation in the Consolidated Statements of Shareholders' Equity if an excess tax benefit is realized. In addition, the Company recognizes the indirect effects of share-based compensation on R&D tax credits, foreign tax credits and domestic manufacturing deductions in the Consolidated Statements of Operations. Further information regarding share-based compensation can be found in Note 9, "Benefit Plans."

Income Taxes

The provision for income taxes is computed using the asset and liability method, under which deferred tax assets and liabilities are recognized for the expected future tax consequences of temporary differences between the financial reporting and tax bases of assets and liabilities and for operating losses and tax credit carryforwards. Deferred tax assets and liabilities are measured using the currently enacted tax rates that apply to taxable income in effect for the years in which those tax assets and liabilities are expected to be realized or settled. The Company records a valuation allowance to reduce deferred tax assets to the amount that is believed more likely than not to be realized.

The Company recognizes the tax benefit from an uncertain tax position only if it is more likely than not the tax position will be sustained on examination by the taxing authorities, based on the technical merits of the position. The tax benefits recognized in the financial statements from such positions are then measured based on the largest benefit that has a greater than 50% likelihood of being realized upon settlement. See Note 5, "Income Taxes" for additional information.

Earnings Per Share

Basic earnings per share is computed by dividing income available to common shareholders by the weighted-average number of shares of common stock outstanding during the period. Diluted earnings per share is computed by dividing income available to common shareholders by the weighted-average number of shares of common stock outstanding during the period increased to include the number of additional shares of common stock that would have been outstanding if the potentially dilutive securities had been issued. Potentially dilutive securities include outstanding stock options, shares to be purchased under the Company's employee stock purchase plan, unvested restricted stock and unvested RSUs. The dilutive effect of potentially dilutive securities is reflected in diluted earnings per share by application of the treasury stock method. Under the treasury stock method, an increase in the fair market value of the Company's common stock can result in a greater dilutive effect from potentially dilutive securities.

The following table shows the computation of basic and diluted earnings per share for 2015, 2014 and 2013 (net income in millions and shares in thousands):

	2015	2014	2013
Numerator:			
Net income	$ 53,394	$ 39,510	$ 37,037
Denominator:			
Weighted-average shares outstanding	5,753,421	6,085,572	6,477,320
Effect of dilutive securities	39,648	37,091	44,314
Weighted-average diluted shares	5,793,069	6,122,663	6,521,634
Basic earnings per share	$ 9.28	$ 6.49	$ 5.72
Diluted earnings per share	$ 9.22	$ 6.45	$ 5.68

Potentially dilutive securities whose effect would have been antidilutive are excluded from the computation of diluted earnings per share.

Financial Instruments

Cash Equivalents and Marketable Securities

All highly liquid investments with maturities of three months or less at the date of purchase are classified as cash equivalents. The Company's marketable debt and equity securities have been classified and accounted for as available-for-sale. Management determines the appropriate classification of its investments at the time of purchase and reevaluates the classifications at each balance sheet date. The Company classifies its marketable debt securities as either short-term or long-term based on each instrument's underlying contractual maturity date. Marketable debt securities with maturities of 12 months or less are classified as short-term and marketable debt securities with maturities greater than 12 months are classified as long-term. Marketable equity securities, including mutual funds, are classified as either short-term or long-term based on the nature of each security and its availability for use in current operations. The Company's marketable debt and equity securities are carried at fair value, with unrealized gains and losses, net of taxes, reported as a component of accumulated other comprehensive income ("AOCI") in shareholders' equity, with the exception of unrealized losses believed to be other-than-temporary which are reported in earnings in the current period. The cost of securities sold is based upon the specific identification method.

Derivative Financial Instruments

The Company accounts for its derivative instruments as either assets or liabilities and carries them at fair value.

For derivative instruments that hedge the exposure to variability in expected future cash flows that are designated as cash flow hedges, the effective portion of the gain or loss on the derivative instrument is reported as a component of AOCI in shareholders' equity and reclassified into earnings in the same period or periods during which the hedged transaction affects earnings. The ineffective portion of the gain or loss on the derivative instrument, if any, is recognized in earnings in the current period. To receive hedge accounting treatment, cash flow hedges must be highly effective in offsetting changes to expected future cash flows on hedged transactions. For options designated as cash flow hedges, changes in the time value are excluded from the assessment of hedge effectiveness and are recognized in earnings.

For derivative instruments that hedge the exposure to changes in the fair value of an asset or a liability and that are designated as fair value hedges, both the net gain or loss on the derivative instrument as well as the offsetting gain or loss on the hedged item are recognized in earnings in the current period.

For derivative instruments and foreign currency debt that hedge the exposure to changes in foreign currency exchange rates used for translation of the net investment in a foreign operation and that are designated as a net investment hedge, the net gain or loss on the effective portion of the derivative instrument is reported in the same manner as a foreign currency translation adjustment. For forward exchange contracts designated as net investment hedges, the Company excludes changes in fair value relating to changes in the forward carry component from its definition of effectiveness. Accordingly, any gains or losses related to this forward carry component are recognized in earnings in the current period.

Derivatives that do not qualify as hedges are adjusted to fair value through earnings in the current period.

Allowance for Doubtful Accounts

The Company records its allowance for doubtful accounts based upon its assessment of various factors, including historical experience, age of the accounts receivable balances, credit quality of the Company's customers, current economic conditions and other factors that may affect the customers' ability to pay.

Inventories

Inventories are stated at the lower of cost, computed using the first-in, first-out method and net realizable value. Any adjustments to reduce the cost of inventories to their net realizable value are recognized in earnings in the current period. As of September 26, 2015 and September 27, 2014, the Company's inventories consist primarily of finished goods.

Property, Plant and Equipment

Property, plant and equipment are stated at cost. Depreciation is computed by use of the straight-line method over the estimated useful lives of the assets, which for buildings is the lesser of 30 years or the remaining life of the underlying building; between one to five years for machinery and equipment, including product tooling and manufacturing process equipment; and the shorter of lease terms or ten years for leasehold improvements. The Company capitalizes eligible costs to acquire or develop internal-use software that are incurred subsequent to the preliminary project stage. Capitalized costs related to internal-use software are amortized using the straight-line method over the estimated useful lives of the assets, which range from three to five years. Depreciation and amortization expense on property and equipment was $9.2 billion, $6.9 billion and $5.8 billion during 2015, 2014 and 2013, respectively.

Long-Lived Assets Including Goodwill and Other Acquired Intangible Assets

The Company reviews property, plant and equipment, inventory component prepayments and certain identifiable intangibles, excluding goodwill, for impairment. Long-lived assets are reviewed for impairment whenever events or changes in circumstances indicate the carrying amount of an asset may not be recoverable. Recoverability of these assets is measured by comparison of their carrying amounts to future undiscounted cash flows the assets are expected to generate. If property, plant and equipment, inventory component prepayments and certain identifiable intangibles are considered to be impaired, the impairment to be recognized equals the amount by which the carrying value of the assets exceeds its fair value.

The Company does not amortize goodwill and intangible assets with indefinite useful lives, rather such assets are required to be tested for impairment at least annually or sooner whenever events or changes in circumstances indicate that the assets may be impaired. The Company performs its goodwill and intangible asset impairment tests in the fourth quarter of each year. The Company did not recognize any impairment charges related to goodwill or indefinite lived intangible assets during 2015, 2014 and 2013. The Company established reporting units based on its current reporting structure. For purposes of testing goodwill for impairment, goodwill has been allocated to these reporting units to the extent it relates to each reporting unit. In 2015 and 2014, the Company's goodwill was primarily allocated to the Americas and Europe reporting units.

The Company amortizes its intangible assets with definite useful lives over their estimated useful lives and reviews these assets for impairment. The Company typically amortizes its acquired intangible assets with definite useful lives over periods from three to seven years.

Fair Value Measurements

The Company applies fair value accounting for all financial assets and liabilities and non-financial assets and liabilities that are recognized or disclosed at fair value in the financial statements on a recurring basis. The Company defines fair value as the price that would be received from selling an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. When determining the fair value measurements for assets and liabilities, which are required to be recorded at fair value, the Company considers the principal or most advantageous market in which the Company would transact and the market-based risk measurements or assumptions that market participants would use in pricing the asset or liability, such as risks inherent in valuation techniques, transfer restrictions and credit risk. Fair value is estimated by applying the following hierarchy, which prioritizes the inputs used to measure fair value into three levels and bases the categorization within the hierarchy upon the lowest level of input that is available and significant to the fair value measurement:

Level 1 – Quoted prices in active markets for identical assets or liabilities.

Level 2 – Observable inputs other than quoted prices in active markets for identical assets and liabilities, quoted prices for identical or similar assets or liabilities in inactive markets, or other inputs that are observable or can be corroborated by observable market data for substantially the full term of the assets or liabilities.

Level 3 – Inputs that are generally unobservable and typically reflect management's estimate of assumptions that market participants would use in pricing the asset or liability.

The Company's valuation techniques used to measure the fair value of money market funds and certain marketable equity securities were derived from quoted prices in active markets for identical assets or liabilities. The valuation techniques used to measure the fair value of the Company's debt instruments and all other financial instruments, all of which have counterparties with high credit ratings, were valued based on quoted market prices or model driven valuations using significant inputs derived from or corroborated by observable market data.

In accordance with the fair value accounting requirements, companies may choose to measure eligible financial instruments and certain other items at fair value. The Company has not elected the fair value option for any eligible financial instruments.

Foreign Currency Translation and Remeasurement

The Company translates the assets and liabilities of its non-U.S. dollar functional currency subsidiaries into U.S. dollars using exchange rates in effect at the end of each period. Revenue and expenses for these subsidiaries are translated using rates that approximate those in effect during the period. Gains and losses from these translations are recognized in foreign currency translation included in AOCI in shareholders' equity. The Company's subsidiaries that use the U.S. dollar as their functional currency remeasure monetary assets and liabilities at exchange rates in effect at the end of each period, and inventories, property and nonmonetary assets and liabilities at historical rates.

Note 2 – Financial Instruments

Cash, Cash Equivalents and Marketable Securities

The following tables show the Company's cash and available-for-sale securities' adjusted cost, gross unrealized gains, gross unrealized losses and fair value by significant investment category recorded as cash and cash equivalents or short- or long-term marketable securities as of September 26, 2015 and September 27, 2014 (in millions):

	2015						
	Adjusted Cost	Unrealized Gains	Unrealized Losses	Fair Value	Cash and Cash Equivalents	Short-Term Marketable Securities	Long-Term Marketable Securities
Cash	$ 11,389	$ 0	$ 0	$ 11,389	$ 11,389	$ 0	$ 0
Level 1:							
Money market funds	1,798	0	0	1,798	1,798	0	0
Mutual funds	1,772	0	(144)	1,628	0	1,628	0
Subtotal	3,570	0	(144)	3,426	1,798	1,628	0
Level 2:							
U.S. Treasury securities	34,902	181	(1)	35,082	0	3,498	31,584
U.S. agency securities	5,864	14	0	5,878	841	767	4,270
Non-U.S. government securities	6,356	45	(167)	6,234	43	135	6,056
Certificates of deposit and time deposits	4,347	0	0	4,347	2,065	1,405	877
Commercial paper	6,016	0	0	6,016	4,981	1,035	0
Corporate securities	116,908	242	(985)	116,165	3	11,948	104,214
Municipal securities	947	5	0	952	0	48	904
Mortgage- and asset-backed securities	16,121	87	(31)	16,177	0	17	16,160
Subtotal	191,461	574	(1,184)	190,851	7,933	18,853	164,065
Total	$ 206,420	$ 574	$ (1,328)	$ 205,666	$ 21,120	$ 20,481	$ 164,065

	2014						
	Adjusted Cost	Unrealized Gains	Unrealized Losses	Fair Value	Cash and Cash Equivalents	Short-Term Marketable Securities	Long-Term Marketable Securities
Cash	$ 10,232	$ 0	$ 0	$ 10,232	$ 10,232	$ 0	$ 0
Level 1:							
Money market funds	1,546	0	0	1,546	1,546	0	0
Mutual funds	2,531	1	(132)	2,400	0	2,400	0
Subtotal	4,077	1	(132)	3,946	1,546	2,400	0
Level 2:							
U.S. Treasury securities	23,140	15	(9)	23,146	12	607	22,527
U.S. agency securities	7,373	3	(11)	7,365	652	157	6,556
Non-U.S. government securities	6,925	69	(69)	6,925	0	204	6,721
Certificates of deposit and time deposits	3,832	0	0	3,832	1,230	1,233	1,369
Commercial paper	475	0	0	475	166	309	0
Corporate securities	85,431	296	(241)	85,486	6	6,298	79,182
Municipal securities	940	8	0	948	0	0	948
Mortgage- and asset-backed securities	12,907	26	(49)	12,884	0	25	12,859
Subtotal	141,023	417	(379)	141,061	2,066	8,833	130,162
Total	$ 155,332	$ 418	$ (511)	$ 155,239	$ 13,844	$ 11,233	$ 130,162

The Company may sell certain of its marketable securities prior to their stated maturities for strategic reasons including, but not limited to, anticipation of credit deterioration and duration management. The maturities of the Company's long-term marketable securities generally range from one to five years.

As of September 26, 2015, the Company considers the declines in market value of its marketable securities investment portfolio to be temporary in nature and does not consider any of its investments other-than-temporarily impaired. The Company typically invests in highly-rated securities, and its investment policy generally limits the amount of credit exposure to any one issuer. The policy generally requires investments to be investment grade, with the primary objective of minimizing the potential risk of principal loss. Fair values were determined for each individual security in the investment portfolio. When evaluating an investment for other-than-temporary impairment the Company reviews factors such as the length of time and extent to which fair value has been below its cost basis, the financial condition of the issuer and any changes thereto, changes in market interest rates and the Company's intent to sell, or whether it is more likely than not it will be required to sell the investment before recovery of the investment's cost basis.

Derivative Financial Instruments

The Company may use derivatives to partially offset its business exposure to foreign currency and interest rate risk on expected future cash flows, on net investments in certain foreign subsidiaries and on certain existing assets and liabilities. However, the Company may choose not to hedge certain exposures for a variety of reasons including, but not limited to, accounting considerations and the prohibitive economic cost of hedging particular exposures. There can be no assurance the hedges will offset more than a portion of the financial impact resulting from movements in foreign currency exchange or interest rates.

To help protect gross margins from fluctuations in foreign currency exchange rates, certain of the Company's subsidiaries whose functional currency is the U.S. dollar may hedge a portion of forecasted foreign currency revenue, and subsidiaries whose functional currency is not the U.S. dollar and who sell in local currencies may hedge a portion of forecasted inventory purchases not denominated in the subsidiaries' functional currencies. The Company may enter into forward contracts, option contracts or other instruments to manage this risk and may designate these instruments as cash flow hedges. The Company typically hedges portions of its forecasted foreign currency exposure associated with revenue and inventory purchases, typically for up to 12 months.

To help protect the net investment in a foreign operation from adverse changes in foreign currency exchange rates, the Company may enter into foreign currency forward and option contracts to offset the changes in the carrying amounts of these investments due to fluctuations in foreign currency exchange rates. In addition, the Company may use non-derivative financial instruments, such as its foreign currency-denominated debt, as economic hedges of its net investments in certain foreign subsidiaries. In both of these cases, the Company designates these instruments as net investment hedges.

The Company may also enter into non-designated foreign currency contracts to partially offset the foreign currency exchange gains and losses generated by the re-measurement of certain assets and liabilities denominated in non-functional currencies.

The Company may enter into interest rate swaps, options, or other instruments to manage interest rate risk. These instruments may offset a portion of changes in income or expense, or changes in fair value of the Company's term debt or investments. The Company designates these instruments as either cash flow or fair value hedges. The Company's hedged interest rate transactions as of September 26, 2015 are expected to be recognized within 10 years.

Cash Flow Hedges

The effective portions of cash flow hedges are recorded in AOCI until the hedged item is recognized in earnings. Deferred gains and losses associated with cash flow hedges of foreign currency revenue are recognized as a component of net sales in the same period as the related revenue is recognized, and deferred gains and losses related to cash flow hedges of inventory purchases are recognized as a component of cost of sales in the same period as the related costs are recognized. Deferred gains and losses associated with cash flow hedges of interest income or expense are recognized in other income/(expense), net in the same period as the related income or expense is recognized. The ineffective portions and amounts excluded from the effectiveness testing of cash flow hedges are recognized in other income/(expense), net.

Derivative instruments designated as cash flow hedges must be de-designated as hedges when it is probable the forecasted hedged transaction will not occur in the initially identified time period or within a subsequent two-month time period. Deferred gains and losses in AOCI associated with such derivative instruments are reclassified immediately into other income/(expense), net. Any subsequent changes in fair value of such derivative instruments are reflected in other income/(expense), net unless they are re-designated as hedges of other transactions.

Net Investment Hedges

The effective portions of net investment hedges are recorded in other comprehensive income ("OCI") as a part of the cumulative translation adjustment. The ineffective portions and amounts excluded from the effectiveness testing of net investment hedges are recognized in other income/(expense), net.

Fair Value Hedges

Gains and losses related to changes in fair value hedges are recognized in earnings along with a corresponding loss or gain related to the change in value of the underlying hedged item.

Non-Designated Derivatives

Derivatives that are not designated as hedging instruments are adjusted to fair value through earnings in the financial statement line item to which the derivative relates.

The Company records all derivatives in the Consolidated Balance Sheets at fair value. The Company's accounting treatment for these derivative instruments is based on its hedge designation. The following tables show the Company's derivative instruments at gross fair value as of September 26, 2015 and September 27, 2014 (in millions):

	2015		
	Fair Value of Derivatives Designated as Hedge Instruments	**Fair Value of Derivatives Not Designated as Hedge Instruments**	**Total Fair Value**
Derivative assets [1]:			
Foreign exchange contracts	$ 1,442	$ 109	$ 1,551
Interest rate contracts	$ 394	$ 0	$ 394
Derivative liabilities [2]:			
Foreign exchange contracts	$ 905	$ 94	$ 999
Interest rate contracts	$ 13	$ 0	$ 13

	2014		
	Fair Value of Derivatives Designated as Hedge Instruments	Fair Value of Derivatives Not Designated as Hedge Instruments	Total Fair Value
Derivative assets [(1)]:			
Foreign exchange contracts	$ 1,332	$ 222	$ 1,554
Interest rate contracts	$ 81	$ 0	$ 81
Derivative liabilities [(2)]:			
Foreign exchange contracts	$ 41	$ 40	$ 81

[(1)] The fair value of derivative assets is measured using Level 2 fair value inputs and is recorded as other current assets in the Consolidated Balance Sheets.

[(2)] The fair value of derivative liabilities is measured using Level 2 fair value inputs and is recorded as accrued expenses in the Consolidated Balance Sheets.

The following table shows the pre-tax gains and losses of the Company's derivative and non-derivative instruments designated as cash flow, net investment and fair value hedges on OCI and the Consolidated Statements of Operations for 2015, 2014 and 2013 (in millions):

	2015	2014	2013
Gains/(Losses) recognized in OCI – effective portion:			
Cash flow hedges:			
Foreign exchange contracts	$ 3,592	$ 1,750	$ 891
Interest rate contracts	(111)	(15)	12
Total	$ 3,481	$ 1,735	$ 903
Net investment hedges:			
Foreign exchange contracts	$ 167	$ 53	$ 143
Foreign currency debt	(71)	0	0
Total	$ 96	$ 53	$ 143
Gains/(Losses) reclassified from AOCI into net income – effective portion:			
Cash flow hedges:			
Foreign exchange contracts	$ 4,092	$ (154)	$ 676
Interest rate contracts	(17)	(16)	(6)
Total	$ 4,075	$ (170)	$ 670
Gains/(Losses) on derivative instruments:			
Fair value hedges:			
Interest rate contracts	$ 337	$ 39	$ 0
Gains/(Losses) related to hedged items:			
Fair value hedges:			
Interest rate contracts	$ (337)	$ (39)	$ 0

The following table shows the notional amounts of the Company's outstanding derivative instruments and credit risk amounts associated with outstanding or unsettled derivative instruments as of September 26, 2015 and September 27, 2014 (in millions):

	2015		2014	
	Notional Amount	Credit Risk Amount	Notional Amount	Credit Risk Amount
Instruments designated as accounting hedges:				
Foreign exchange contracts	$ 70,054	$ 1,385	$ 42,945	$ 1,333
Interest rate contracts	$ 18,750	$ 394	$ 12,000	$ 89
Instruments not designated as accounting hedges:				
Foreign exchange contracts	$ 49,190	$ 109	$ 38,510	$ 222

The notional amounts for outstanding derivative instruments provide one measure of the transaction volume outstanding and do not represent the amount of the Company's exposure to credit or market loss. The credit risk amounts represent the Company's gross exposure to potential accounting loss on derivative instruments that are outstanding or unsettled if all counterparties failed to perform according to the terms of the contract, based on then-current currency or interest rates at each respective date. The Company's exposure to credit loss and market risk will vary over time as currency and interest rates change. Although the table above reflects the notional and credit risk amounts of the Company's derivative instruments, it does not reflect the gains or losses associated with the exposures and transactions that the instruments are intended to hedge. The amounts ultimately realized upon settlement of these financial instruments, together with the gains and losses on the underlying exposures, will depend on actual market conditions during the remaining life of the instruments.

The Company generally enters into master netting arrangements, which are designed to reduce credit risk by permitting net settlement of transactions with the same counterparty. To further limit credit risk, the Company generally enters into collateral security arrangements that provide for collateral to be received or posted when the net fair value of certain financial instruments fluctuates from contractually established thresholds. The Company presents its derivative assets and derivative liabilities at their gross fair values in its Consolidated Balance Sheets. The net cash collateral received by the Company related to derivative instruments under its collateral security arrangements was $1.0 billion as of September 26, 2015 and $2.1 billion as of September 27, 2014.

Under master netting arrangements with the respective counterparties to the Company's derivative contracts, the Company is allowed to net settle transactions with a single net amount payable by one party to the other. As of September 26, 2015 and September 27, 2014, the potential effects of these rights of set-off associated with the Company's derivative contracts, including the effects of collateral, would be a reduction to both derivative assets and derivative liabilities of $2.2 billion and $1.6 billion, respectively, resulting in net derivative liabilities of $78 million and $549 million, respectively.

Accounts Receivable

Trade Receivables

The Company has considerable trade receivables outstanding with its third-party cellular network carriers, wholesalers, retailers, value-added resellers, small and mid-sized businesses and education, enterprise and government customers. The Company generally does not require collateral from its customers; however, the Company will require collateral in certain instances to limit credit risk. In addition, when possible, the Company attempts to limit credit risk on trade receivables with credit insurance for certain customers or by requiring third-party financing, loans or leases to support credit exposure. These credit-financing arrangements are directly between the third-party financing company and the end customer. As such, the Company generally does not assume any recourse or credit risk sharing related to any of these arrangements.

As of September 26, 2015, the Company had one customer that represented 10% or more of total trade receivables, which accounted for 12%. As of September 27, 2014, the Company had two customers that represented 10% or more of total trade receivables, one of which accounted for 16% and the other 13%. The Company's cellular network carriers accounted for 71% and 72% of trade receivables as of September 26, 2015 and September 27, 2014, respectively.

Vendor Non-Trade Receivables

The Company has non-trade receivables from certain of its manufacturing vendors resulting from the sale of components to these vendors who manufacture sub-assemblies or assemble final products for the Company. The Company purchases these components directly from suppliers. Vendor non-trade receivables from three of the Company's vendors accounted for 38%, 18% and 14% of total vendor non-trade receivables as of September 26, 2015 and three of the Company's vendors accounted for 51%, 16% and 14% of total vendor non-trade receivables as of September 27, 2014.

Note 3 – Consolidated Financial Statement Details

The following tables show the Company's consolidated financial statement details as of September 26, 2015 and September 27, 2014 (in millions):

Property, Plant and Equipment, Net

	2015	2014
Land and buildings	$ 6,956	$ 4,863
Machinery, equipment and internal-use software	37,038	29,639
Leasehold improvements	5,263	4,513
Gross property, plant and equipment	49,257	39,015
Accumulated depreciation and amortization	(26,786)	(18,391)
Total property, plant and equipment, net	$ 22,471	$ 20,624

Other Non-Current Liabilities

	2015	2014
Deferred tax liabilities	$ 24,062	$ 20,259
Other non-current liabilities	9,365	4,567
Total other non-current liabilities	$ 33,427	$ 24,826

Other Income/(Expense), Net

The following table shows the detail of other income/(expense), net for 2015, 2014 and 2013 (in millions):

	2015	2014	2013
Interest and dividend income	$ 2,921	$ 1,795	$ 1,616
Interest expense	(733)	(384)	(136)
Other expense, net	(903)	(431)	(324)
Total other income/(expense), net	$ 1,285	$ 980	$ 1,156

Note 4 – Goodwill and Other Intangible Assets

On July 31, 2014, the Company completed the acquisitions of Beats Music, LLC, which offers a subscription streaming music service, and Beats Electronics, LLC, which makes Beats® headphones, speakers and audio software (collectively, "Beats"). The total purchase price consideration for these acquisitions was $2.6 billion, which consisted primarily of cash, of which $2.2 billion was allocated to goodwill, $636 million to acquired intangible assets and $258 million to net liabilities assumed. Concurrent with the close of the acquisitions, the Company repaid $295 million of existing Beats outstanding debt to third-party creditors. In conjunction with the Beats acquisitions, the Company issued approximately 5.1 million shares of its common stock to certain former equity holders of Beats. The restricted stock was valued at approximately $485 million based on the Company's common stock on the acquisition date. The majority of these shares, valued at approximately $417 million, will vest over time based on continued employment with Apple.

The Company also completed various other business acquisitions during 2014 for an aggregate cash consideration, net of cash acquired, of $957 million, of which $828 million was allocated to goodwill, $257 million to acquired intangible assets and $128 million to net liabilities assumed.

The Company's acquired intangible assets with definite useful lives primarily consist of patents and licenses and are amortized over periods typically from three to seven years. The following table summarizes the components of gross and net intangible asset balances as of September 26, 2015 and September 27, 2014 (in millions):

	2015			2014		
	Gross Carrying Amount	Accumulated Amortization	Net Carrying Amount	Gross Carrying Amount	Accumulated Amortization	Net Carrying Amount
Definite-lived and amortizable acquired intangible assets	$ 8,125	$ (4,332)	$ 3,793	$ 7,127	$ (3,085)	$ 4,042
Indefinite-lived and non-amortizable acquired intangible assets	100	0	100	100	0	100
Total acquired intangible assets	$ 8,225	$ (4,332)	$ 3,893	$ 7,227	$ (3,085)	$ 4,142

Amortization expense related to acquired intangible assets was $1.3 billion, $1.1 billion and $960 million in 2015, 2014 and 2013, respectively. As of September 26, 2015, the remaining weighted-average amortization period for acquired intangible assets is 3.6 years. The expected annual amortization expense related to acquired intangible assets as of September 26, 2015, is as follows (in millions):

2016	$ 1,288
2017	1,033
2018	786
2019	342
2020	166
Thereafter	178
Total	$ 3,793

Note 5 – Income Taxes

The provision for income taxes for 2015, 2014 and 2013, consisted of the following (in millions):

	2015	2014	2013
Federal:			
Current	$ 11,730	$ 8,624	$ 9,334
Deferred	3,408	3,183	1,878
	15,138	11,807	11,212
State:			
Current	1,265	855	1,084
Deferred	(220)	(178)	(311)
	1,045	677	773
Foreign:			
Current	4,744	2,147	1,559
Deferred	(1,806)	(658)	(426)
	2,938	1,489	1,133
Provision for income taxes	$ 19,121	$ 13,973	$ 13,118

The foreign provision for income taxes is based on foreign pre-tax earnings of $47.6 billion, $33.6 billion and $30.5 billion in 2015, 2014 and 2013, respectively. The Company's consolidated financial statements provide for any related tax liability on undistributed earnings that the Company does not intend to be indefinitely reinvested outside the U.S. Substantially all of the Company's undistributed international earnings intended to be indefinitely reinvested in operations outside the U.S. were generated by subsidiaries organized in Ireland, which has a statutory tax rate of 12.5%. As of September 26, 2015, U.S. income taxes have not been provided on a cumulative total of $91.5 billion of such earnings. The amount of unrecognized deferred tax liability related to these temporary differences is estimated to be $30.0 billion.

As of September 26, 2015 and September 27, 2014, $186.9 billion and $137.1 billion, respectively, of the Company's cash, cash equivalents and marketable securities were held by foreign subsidiaries and are generally based in U.S. dollar-denominated holdings. Amounts held by foreign subsidiaries are generally subject to U.S. income taxation on repatriation to the U.S.

A reconciliation of the provision for income taxes, with the amount computed by applying the statutory federal income tax rate (35% in 2015, 2014 and 2013) to income before provision for income taxes for 2015, 2014 and 2013, is as follows (dollars in millions):

	2015	2014	2013
Computed expected tax	$ 25,380	$ 18,719	$ 17,554
State taxes, net of federal effect	680	469	508
Indefinitely invested earnings of foreign subsidiaries	(6,470)	(4,744)	(4,614)
Domestic production activities deduction	(426)	(495)	(308)
Research and development credit, net	(171)	(88)	(287)
Other	128	112	265
Provision for income taxes	$ 19,121	$ 13,973	$ 13,118
Effective tax rate	26.4%	26.1%	26.2%

The Company's income taxes payable have been reduced by the tax benefits from employee stock plan awards. For stock options, the Company receives an income tax benefit calculated as the tax effect of the difference between the fair market value of the stock issued at the time of the exercise and the exercise price. For RSUs, the Company receives an income tax benefit upon the award's vesting equal to the tax effect of the underlying stock's fair market value. The Company had net excess tax benefits from equity awards of $748 million, $706 million and $643 million in 2015, 2014 and 2013, respectively, which were reflected as increases to common stock.

As of September 26, 2015 and September 27, 2014, the significant components of the Company's deferred tax assets and liabilities were (in millions):

	2015	2014
Deferred tax assets:		
Accrued liabilities and other reserves	$ 4,205	$ 3,326
Basis of capital assets and investments	2,238	898
Deferred revenue	1,941	1,787
Deferred cost sharing	667	0
Share-based compensation	575	454
Unrealized losses	564	130
Other	721	227
Total deferred tax assets, net of valuation allowance of $0	10,911	6,822
Deferred tax liabilities:		
Unremitted earnings of foreign subsidiaries	26,868	21,544
Other	303	398
Total deferred tax liabilities	27,171	21,942
Net deferred tax liabilities	$ (16,260)	$ (15,120)

Deferred tax assets and liabilities reflect the effects of tax losses, credits and the future income tax effects of temporary differences between the consolidated financial statement carrying amounts of existing assets and liabilities and their respective tax bases and are measured using enacted tax rates that apply to taxable income in the years in which those temporary differences are expected to be recovered or settled.

Uncertain Tax Positions

Tax positions are evaluated in a two-step process. The Company first determines whether it is more likely than not that a tax position will be sustained upon examination. If a tax position meets the more-likely-than-not recognition threshold it is then measured to determine the amount of benefit to recognize in the financial statements. The tax position is measured as the largest amount of benefit that is greater than 50% likely of being realized upon ultimate settlement. The Company classifies gross interest and penalties and unrecognized tax benefits that are not expected to result in payment or receipt of cash within one year as non-current liabilities in the Consolidated Balance Sheets.

As of September 26, 2015, the total amount of gross unrecognized tax benefits was $6.9 billion, of which $2.5 billion, if recognized, would affect the Company's effective tax rate. As of September 27, 2014, the total amount of gross unrecognized tax benefits was $4.0 billion, of which $1.4 billion, if recognized, would affect the Company's effective tax rate.

The aggregate changes in the balance of gross unrecognized tax benefits, which excludes interest and penalties, for 2015, 2014 and 2013, is as follows (in millions):

	2015	2014	2013
Beginning Balance	$ 4,033	$ 2,714	$ 2,062
Increases related to tax positions taken during a prior year	2,056	1,295	745
Decreases related to tax positions taken during a prior year	(345)	(280)	(118)
Increases related to tax positions taken during the current year	1,278	882	626
Decreases related to settlements with taxing authorities	(109)	(574)	(592)
Decreases related to expiration of statute of limitations	(13)	(4)	(9)
Ending Balance	$ 6,900	$ 4,033	$ 2,714

The Company includes interest and penalties related to unrecognized tax benefits within the provision for income taxes. As of September 26, 2015 and September 27, 2014, the total amount of gross interest and penalties accrued was $1.3 billion and $630 million, respectively, which is classified as non-current liabilities in the Consolidated Balance Sheets. In connection with tax matters, the Company recognized interest and penalty expense in 2015, 2014 and 2013 of $709 million, $40 million and $189 million, respectively.

The Company is subject to taxation and files income tax returns in the U.S. federal jurisdiction and in many state and foreign jurisdictions. The U.S. Internal Revenue Service (the "IRS") is currently examining the years 2010 through 2012, and all years prior to 2010 are closed. In addition, the Company is subject to audits by state, local and foreign tax authorities. In major states and major foreign jurisdictions, the years subsequent to 2003 generally remain open and could be subject to examination by the taxing authorities.

Management believes that an adequate provision has been made for any adjustments that may result from tax examinations. However, the outcome of tax audits cannot be predicted with certainty. If any issues addressed in the Company's tax audits are resolved in a manner not consistent with management's expectations, the Company could be required to adjust its provision for income taxes in the period such resolution occurs. Although timing of the resolution and/or closure of audits is not certain, the Company does not believe it is reasonably possible that its unrecognized tax benefits would materially change in the next 12 months.

On June 11, 2014, the European Commission issued an opening decision initiating a formal investigation against Ireland for alleged state aid to the Company. The opening decision concerns the allocation of profits for taxation purposes of the Irish branches of two subsidiaries of the Company. The Company believes the European Commission's assertions are without merit. If the European Commission were to conclude against Ireland, the European Commission could require Ireland to recover from the Company past taxes covering a period of up to 10 years reflective of the disallowed state aid. While such amount could be material, as of September 26, 2015 the Company is unable to estimate the impact.

Note 6 – Debt

Commercial Paper

In 2014, the Board of Directors authorized the Company to issue unsecured short-term promissory notes ("Commercial Paper") pursuant to a commercial paper program. The Company intends to use net proceeds from the commercial paper program for general corporate purposes, including dividends and share repurchases. As of September 26, 2015 and September 27, 2014, the Company had $8.5 billion and $6.3 billion of Commercial Paper outstanding, respectively, with a weighted-average interest rate of 0.14% and 0.12%, respectively, and maturities generally less than nine months.

The following table provides a summary of cash flows associated with the issuance and maturities of Commercial Paper for 2015 and 2014 (in millions):

	2015	2014
Maturities less than 90 days:		
Proceeds from (repayments of) commercial paper, net	$ 5,293	$ 1,865
Maturities greater than 90 days:		
Proceeds from commercial paper	3,851	4,771
Repayments of commercial paper	(6,953)	(330)
Maturities greater than 90 days, net	(3,102)	4,441
Total change in commercial paper, net	$ 2,191	$ 6,306

Long-Term Debt

As of September 26, 2015, the Company had outstanding floating- and fixed-rate notes with varying maturities for an aggregate principal amount of $55.7 billion (collectively the "Notes"). The Notes are senior unsecured obligations, and interest is payable in arrears, quarterly for the U.S. dollar-denominated and Australian dollar-denominated floating-rate notes, semi-annually for the U.S. dollar-denominated, Australian dollar-denominated, British pound-denominated and Japanese yen-denominated fixed-rate notes and annually for the euro-denominated and Swiss franc-denominated fixed-rate notes.

The following table provides a summary of the Company's term debt as of September 26, 2015 and September 27, 2014:

		2015		2014	
	Maturities	Amount (in millions)	Effective Interest Rate	Amount (in millions)	Effective Interest Rate
2013 debt issuance of $17.0 billion:					
Floating-rate notes	2016 – 2018	$ 3,000	0.51% – 1.10%	$ 3,000	0.51% – 1.10%
Fixed-rate 0.45% – 3.85% notes	2016 – 2043	14,000	0.51% – 3.91%	14,000	0.51% – 3.91%
2014 debt issuance of $12.0 billion:					
Floating-rate notes	2017 – 2019	2,000	0.37% – 0.60%	2,000	0.31% – 0.54%
Fixed-rate 1.05% – 4.45% notes	2017 – 2044	10,000	0.37% – 4.48%	10,000	0.30% – 4.48%
First quarter 2015 euro-denominated debt issuance of €2.8 billion:					
Fixed-rate 1.000% notes	2022	1,558	2.94%	0	0
Fixed-rate 1.625% notes	2026	1,558	3.45%	0	0
Second quarter 2015 debt issuance of $6.5 billion:					
Floating-rate notes	2020	500	0.56%	0	0
Fixed-rate 1.55% notes	2020	1,250	0.56%	0	0
Fixed-rate 2.15% notes	2022	1,250	0.87%	0	0
Fixed-rate 2.50% notes	2025	1,500	2.60%	0	0
Fixed-rate 3.45% notes	2045	2,000	3.58%	0	0
Second quarter 2015 Swiss franc-denominated debt issuance of SFr1.25 billion:					
Fixed-rate 0.375% notes	2024	895	0.28%	0	0
Fixed-rate 0.750% notes	2030	384	0.74%	0	0
Third quarter 2015 debt issuance of $8.0 billion:					
Floating-rate notes	2017	250	0.36%	0	0
Floating-rate notes	2020	500	0.61%	0	0
Fixed-rate 0.900% notes	2017	750	0.35%	0	0
Fixed-rate 2.000% notes	2020	1,250	0.61%	0	0
Fixed-rate 2.700% notes	2022	1,250	0.99%	0	0
Fixed-rate 3.200% notes	2025	2,000	1.22%	0	0
Fixed-rate 4.375% notes	2045	2,000	4.40%	0	0
Third quarter 2015 Japanese yen-denominated debt issuance of ¥250.0 billion:					
Fixed-rate 0.35% notes	2020	2,081	0.35%	0	0
Fourth quarter 2015 British pound-denominated debt issuance of £1.25 billion:					
Fixed-rate 3.05% notes	2029	1,148	3.79%	0	0
Fixed-rate 3.60% notes	2042	766	4.51%	0	0
Fourth quarter 2015 Australian dollar-denominated debt issuance of A$2.25 billion:					
Floating-rate notes	2019	493	1.87%	0	0
Fixed-rate 2.85% notes	2019	282	1.89%	0	0
Fixed-rate 3.70% notes	2022	810	2.79%	0	0
Fourth quarter 2015 euro-denominated debt issuance of €2.0 billion:					
Fixed-rate 1.375% notes	2024	1,113	3.30%	0	0
Fixed-rate 2.000% notes	2027	1,113	3.85%	0	0
Total term debt		55,701		29,000	
Unamortized discount		(114)		(52)	
Hedge accounting fair value adjustments		376		39	
Less: Current portion of long-term debt		(2,500)		0	
Total long-term debt		$ 53,463		$ 28,987	

To manage foreign currency risk associated with the euro-denominated notes issued in the first quarter of 2015 and the British pound-denominated, Australian dollar-denominated and euro-denominated notes issued in the fourth quarter of 2015, the Company entered into currency swaps with an aggregate notional amount of $3.5 billion, $1.9 billion, $1.6 billion and $2.2 billion, respectively, which effectively converted these notes to U.S. dollar-denominated notes.

To manage interest rate risk on the U.S. dollar-denominated fixed-rate notes issued in the second quarter of 2015 and maturing in 2020 and 2022, the Company entered into interest rate swaps with an aggregate notional amount of $2.5 billion. To manage interest rate risk on the U.S. dollar-denominated fixed-rate notes issued in the third quarter of 2015 and maturing in 2017, 2020, 2022 and 2025, the Company entered into interest rate swaps with an aggregate notional amount of $4.3 billion. These interest rate swaps effectively converted the fixed interest rates on the U.S. dollar-denominated notes to a floating interest rate.

As of September 26, 2015, ¥250.0 billion of the Japanese yen-denominated notes was designated as a hedge of the foreign currency exposure of its net investment in a foreign operation. The foreign currency transaction gain or loss on the Japanese yen-denominated debt designated as a hedge is recorded in OCI as a part of the cumulative translation adjustment. As of September 26, 2015, the carrying value of the debt designated as a net investment hedge was $2.1 billion.

For further discussion regarding the Company's use of derivative instruments see the Derivative Financial Instruments section of Note 2, "Financial Instruments."

The effective interest rates for the Notes include the interest on the Notes, amortization of the discount and, if applicable, adjustments related to hedging. The Company recognized $722 million, $381 million and $136 million of interest expense on its term debt for 2015, 2014 and 2013, respectively.

The future principal payments for the Company's Notes as of September 26, 2015 are as follows (in millions):

2016	$ 2,500
2017	3,500
2018	6,000
2019	3,775
2020	5,581
Thereafter	34,345
Total term debt	$ 55,701

As of September 26, 2015 and September 27, 2014, the fair value of the Company's Notes, based on Level 2 inputs, was $54.9 billion and $28.5 billion, respectively.

Note 7 – Shareholders' Equity

Dividends

The Company declared and paid cash dividends per share during the periods presented as follows:

	Dividends Per Share	Amount (in millions)
2015:		
Fourth quarter	$ 0.52	$ 2,950
Third quarter	0.52	2,997
Second quarter	0.47	2,734
First quarter	0.47	2,750
Total cash dividends declared and paid	$ 1.98	$ 11,431
2014:		
Fourth quarter	$ 0.47	$ 2,807
Third quarter	0.47	2,830
Second quarter	0.44	2,655
First quarter	0.44	2,739
Total cash dividends declared and paid	$ 1.82	$ 11,031

Future dividends are subject to declaration by the Board of Directors.

Share Repurchase Program

In the third quarter of 2015, the Company's Board of Directors increased the share repurchase authorization to $140 billion of the Company's common stock, of which $104 billion had been utilized as of September 26, 2015. The Company's share repurchase program does not obligate it to acquire any specific number of shares. Under the program, shares may be repurchased in privately negotiated and/or open market transactions, including under plans complying with Rule 10b5-1 under the Securities Exchange Act of 1934, as amended (the "Exchange Act").

The Company has entered, and in the future may enter, into accelerated share repurchase arrangements ("ASRs") with financial institutions. In exchange for up-front payments, the financial institutions deliver shares of the Company's common stock during the purchase periods of each ASR. The total number of shares ultimately delivered, and therefore the average repurchase price paid per share, is determined at the end of the applicable purchase period of each ASR based on the volume weighted-average price of the Company's common stock during that period. The shares received are retired in the periods they are delivered, and the up-front payments are accounted for as a reduction to shareholders' equity in the Company's Consolidated Balance Sheets in the periods the payments are made. The Company reflects the ASRs as a repurchase of common stock in the period delivered for purposes of calculating earnings per share and as forward contracts indexed to its own common stock. The ASRs met all of the applicable criteria for equity classification, and therefore were not accounted for as derivative instruments.

The following table shows the Company's ASR activity and related information during the years ended September 26, 2015 and September 27, 2014:

	Purchase Period End Date	Number of Shares (in thousands)	Average Repurchase Price Per Share	ASR Amount (in millions)
May 2015 ASR	July 2015	48,293 [1]	$ 124.24	$ 6,000
August 2014 ASR	February 2015	81,525 [2]	$ 110.40	$ 9,000
January 2014 ASR	December 2014	134,247	$ 89.39	$ 12,000
April 2013 ASR	March 2014	172,548	$ 69.55	$ 12,000

[1] Includes 38.3 million shares delivered and retired at the beginning of the purchase period, which began in the third quarter of 2015 and 10.0 million shares delivered and retired at the end of the purchase period, which concluded in the fourth quarter of 2015.

[2] Includes 59.9 million shares delivered and retired at the beginning of the purchase period, which began in the fourth quarter of 2014, 8.3 million net shares delivered and retired in the first quarter of 2015 and 13.3 million shares delivered and retired at the end of the purchase period, which concluded in the second quarter of 2015.

Additionally, the Company repurchased shares of its common stock in the open market, which were retired upon repurchase, during the periods presented as follows:

	Number of Shares (in thousands)	Average Repurchase Price Per Share	Amount (in millions)
2015:			
Fourth quarter	121,802	$ 115.15	$ 14,026
Third quarter	31,231	$ 128.08	4,000
Second quarter	56,400	$ 124.11	7,000
First quarter	45,704	$ 109.40	5,000
Total open market common stock repurchases	255,137		$ 30,026
2014:			
Fourth quarter	81,255	$ 98.46	$ 8,000
Third quarter	58,661	$ 85.23	5,000
Second quarter	79,749	$ 75.24	6,000
First quarter	66,847	$ 74.79	5,000
Total open market common stock repurchases	286,512		$ 24,000

Note 8 – Comprehensive Income

Comprehensive income consists of two components, net income and OCI. OCI refers to revenue, expenses, and gains and losses that under GAAP are recorded as an element of shareholders' equity but are excluded from net income. The Company's OCI consists of foreign currency translation adjustments from those subsidiaries not using the U.S. dollar as their functional currency, net deferred gains and losses on certain derivative instruments accounted for as cash flow hedges and unrealized gains and losses on marketable securities classified as available-for-sale.

The following table shows the pre-tax amounts reclassified from AOCI into the Consolidated Statements of Operations, and the associated financial statement line item, for 2015 and 2014 (in millions):

Comprehensive Income Components	Financial Statement Line Item	2015	2014
Unrealized (gains)/losses on derivative instruments:			
Foreign exchange contracts	Revenue	$ (2,432)	$ 449
	Cost of sales	(2,168)	(295)
	Other income/(expense), net	456	15
Interest rate contracts	Other income/(expense), net	17	16
		(4,127)	185
Unrealized (gains)/losses on marketable securities	Other income/(expense), net	91	(205)
Total amounts reclassified from AOCI		$ (4,036)	$ (20)

The following table shows the changes in AOCI by component for 2015 (in millions):

	Cumulative Foreign Currency Translation	Unrealized Gains/Losses on Derivative Instruments	Unrealized Gains/Losses on Marketable Securities	Total
Balance at September 28, 2013	$ (105)	$ (175)	$ (191)	$ (471)
Other comprehensive income/(loss) before reclassifications	(187)	1,687	438	1,938
Amounts reclassified from AOCI	0	185	(205)	(20)
Tax effect	50	(333)	(82)	(365)
Other comprehensive income/(loss)	(137)	1,539	151	1,553
Balance at September 27, 2014	(242)	1,364	(40)	1,082
Other comprehensive income/(loss) before reclassifications	(612)	3,346	(747)	1,987
Amounts reclassified from AOCI	0	(4,127)	91	(4,036)
Tax effect	201	189	232	622
Other comprehensive income/(loss)	(411)	(592)	(424)	(1,427)
Balance at September 26, 2015	$ (653)	$ 772	$ (464)	$ (345)

Note 9 – Benefit Plans

2014 Employee Stock Plan

In the second quarter of 2014, shareholders approved the 2014 Employee Stock Plan (the “2014 Plan”) and terminated the Company’s authority to grant new awards under the 2003 Employee Stock Plan (the “2003 Plan”). The 2014 Plan provides for broad-based equity grants to employees, including executive officers, and permits the granting of RSUs, stock grants, performance-based awards, stock options and stock appreciation rights, as well as cash bonus awards. RSUs granted under the 2014 Plan generally vest over four years, based on continued employment, and are settled upon vesting in shares of the Company’s common stock on a one-for-one basis. Each share issued with respect to RSUs granted under the 2014 Plan reduces the number of shares available for grant under the plan by two shares. RSUs cancelled and shares withheld to satisfy tax withholding obligations increase the number of shares available for grant under the 2014 Plan utilizing a factor of two times the number of RSUs cancelled or shares withheld. Currently, all RSUs granted under the 2014 Plan have dividend equivalent rights (“DERs”), which entitle holders of RSUs to the same dividend value per share as holders of common stock. DERs are subject to the same vesting and other terms and conditions as the corresponding unvested RSUs. DERs are accumulated and paid when the underlying shares vest. Upon approval of the 2014 Plan, the Company reserved 385 million shares plus the number of shares remaining that were reserved but not issued under the 2003 Plan. Shares subject to outstanding awards under the 2003 Plan that expire, are cancelled or otherwise terminate, or are withheld to satisfy tax withholding obligations with respect to RSUs, will also be available for awards under the 2014 Plan. As of September 26, 2015, approximately 442.9 million shares were reserved for future issuance under the 2014 Plan.

2003 Employee Stock Plan

The 2003 Plan is a shareholder approved plan that provided for broad-based equity grants to employees, including executive officers. The 2003 Plan permitted the granting of incentive stock options, nonstatutory stock options, RSUs, stock appreciation rights, stock purchase rights and performance-based awards. Options granted under the 2003 Plan generally expire seven to ten years after the grant date and generally become exercisable over a period of four years, based on continued employment, with either annual, semi-annual or quarterly vesting. RSUs granted under the 2003 Plan generally vest over two to four years, based on continued employment and are settled upon vesting in shares of the Company’s common stock on a one-for-one basis. All RSUs, other than RSUs held by the Chief Executive Officer, granted under the 2003 Plan have DERs. DERs are subject to the same vesting and other terms and conditions as the corresponding unvested RSUs. DERs are accumulated and paid when the underlying shares vest. In the second quarter of 2014, the Company terminated the authority to grant new awards under the 2003 Plan.

1997 Director Stock Plan

The 1997 Director Stock Plan (the “Director Plan”) is a shareholder approved plan that (i) permits the Company to grant awards of RSUs or stock options to the Company’s non-employee directors, (ii) provides for automatic initial grants of RSUs upon a non-employee director joining the Board of Directors and automatic annual grants of RSUs at each annual meeting of shareholders, and (iii) permits the Board of Directors to prospectively change the relative mixture of stock options and RSUs for the initial and annual award grants and the methodology for determining the number of shares of the Company’s common stock subject to these grants without shareholder approval. Each share issued with respect to RSUs granted under the Director Plan reduces the number of shares available for grant under the plan by two shares. The Director Plan expires November 9, 2019. All RSUs granted under the Director Plan are entitled to DERs. DERs are subject to the same vesting and other terms and conditions as the corresponding unvested RSUs. DERs are accumulated and paid when the underlying shares vest. As of September 26, 2015, approximately 1.2 million shares were reserved for future issuance under the Director Plan.

Rule 10b5-1 Trading Plans

During the fourth quarter of 2015, Section 16 officers Timothy D. Cook, Angela Ahrendts, Luca Maestri, Daniel Riccio, Philip Schiller and Jeffrey Williams had equity trading plans in place in accordance with Rule 10b5-1(c)(1) under the Exchange Act. An equity trading plan is a written document that pre-establishes the amounts, prices and dates (or formula for determining the amounts, prices and dates) of future purchases or sales of the Company’s stock, including shares acquired pursuant to the Company’s employee and director equity plans.

Employee Stock Purchase Plan

The Employee Stock Purchase Plan (the “Purchase Plan”) is a shareholder approved plan under which substantially all employees may purchase the Company’s common stock through payroll deductions at a price equal to 85% of the lower of the fair market values of the stock as of the beginning or the end of six-month offering periods. An employee’s payroll deductions under the Purchase Plan are limited to 10% of the employee’s compensation and employees may not purchase more than $25,000 of stock during any calendar year. As of September 26, 2015, approximately 53.0 million shares were reserved for future issuance under the Purchase Plan.

401(k) Plan

The Company's 401(k) Plan is a deferred salary arrangement under Section 401(k) of the Internal Revenue Code. Under the 401(k) Plan, participating U.S. employees may defer a portion of their pre-tax earnings, up to the IRS annual contribution limit ($18,000 for calendar year 2015). The Company matches 50% to 100% of each employee's contributions, depending on length of service, up to a maximum 6% of the employee's eligible earnings. The Company's matching contributions to the 401(k) Plan were $200 million, $163 million and $135 million in 2015, 2014 and 2013, respectively.

Restricted Stock Units

A summary of the Company's RSU activity and related information for 2015, 2014 and 2013, is as follows:

	Number of RSUs (in thousands)	Weighted-Average Grant Date Fair Value Per Share	Aggregate Intrinsic Value (in millions)
Balance at September 29, 2012	105,037	$ 49.27	
RSUs granted	39,415	$ 78.23	
RSUs vested	(42,291)	$ 45.96	
RSUs cancelled	(8,877)	$ 57.31	
Balance at September 28, 2013	93,284	$ 62.24	
RSUs granted	59,269	$ 74.54	
RSUs vested	(43,111)	$ 57.29	
RSUs cancelled	(5,620)	$ 68.47	
Balance at September 27, 2014	103,822	$ 70.98	
RSUs granted	45,587	$ 105.51	
RSUs vested	(41,684)	$ 71.32	
RSUs cancelled	(6,258)	$ 80.34	
Balance at September 26, 2015	101,467	$ 85.77	$ 11,639

The fair value as of the respective vesting dates of RSUs was $4.8 billion, $3.4 billion and $3.1 billion for 2015, 2014 and 2013, respectively. The majority of RSUs that vested in 2015, 2014 and 2013 were net-share settled such that the Company withheld shares with value equivalent to the employees' minimum statutory obligation for the applicable income and other employment taxes, and remitted the cash to the appropriate taxing authorities. The total shares withheld were approximately 14.1 million, 15.6 million and 15.5 million for 2015, 2014 and 2013, respectively, and were based on the value of the RSUs on their respective vesting dates as determined by the Company's closing stock price. Total payments for the employees' tax obligations to taxing authorities were $1.6 billion, $1.2 billion and $1.1 billion in 2015, 2014 and 2013, respectively, and are reflected as a financing activity within the Consolidated Statements of Cash Flows. These net-share settlements had the effect of share repurchases by the Company as they reduced the number of shares that would have otherwise been issued as a result of the vesting and did not represent an expense to the Company.

Stock Options

The Company had 1.2 million stock options outstanding as of September 26, 2015, with a weighted-average exercise price per share of $15.08 and weighted-average remaining contractual term of 4.1 years, substantially all of which are exercisable. The aggregate intrinsic value of the stock options outstanding as of September 26, 2015 was $120 million, which represents the value of the Company's closing stock price on the last trading day of the period in excess of the weighted-average exercise price multiplied by the number of options outstanding. Total intrinsic value of options at time of exercise was $479 million, $1.5 billion and $1.0 billion for 2015, 2014 and 2013, respectively.

Share-based Compensation

The following table shows a summary of the share-based compensation expense included in the Consolidated Statements of Operations for 2015, 2014 and 2013 (in millions):

	2015	2014	2013
Cost of sales	$ 575	$ 450	$ 350
Research and development	1,536	1,216	917
Selling, general and administrative	1,475	1,197	986
Total share-based compensation expense	$ 3,586	$ 2,863	$ 2,253

The income tax benefit related to share-based compensation expense was $1.2 billion, $1.0 billion and $816 million for 2015, 2014 and 2013, respectively. As of September 26, 2015, the total unrecognized compensation cost related to outstanding stock options, RSUs and restricted stock was $6.8 billion, which the Company expects to recognize over a weighted-average period of 2.7 years.

Note 10 – Commitments and Contingencies

Accrued Warranty and Indemnification

The following table shows changes in the Company’s accrued warranties and related costs for 2015, 2014 and 2013 (in millions):

	2015	2014	2013
Beginning accrued warranty and related costs	$ 4,159	$ 2,967	$ 1,638
Cost of warranty claims	(4,401)	(3,760)	(3,703)
Accruals for product warranty	5,022	4,952	5,032
Ending accrued warranty and related costs	$ 4,780	$ 4,159	$ 2,967

The Company generally does not indemnify end-users of its operating system and application software against legal claims that the software infringes third-party intellectual property rights. Other agreements entered into by the Company sometimes include indemnification provisions under which the Company could be subject to costs and/or damages in the event of an infringement claim against the Company or an indemnified third-party. In the opinion of management, there was not at least a reasonable possibility the Company may have incurred a material loss with respect to indemnification of end-users of its operating system or application software for infringement of third-party intellectual property rights. The Company did not record a liability for infringement costs related to indemnification as of September 26, 2015 or September 27, 2014.

In September 2015, the Company introduced the iPhone Upgrade Program, which is available to customers who purchase an iPhone 6s and 6s Plus in one of its U.S. physical retail stores and activate the purchased iPhone with one of the four national carriers. The iPhone Upgrade Program provides customers the right to trade in that iPhone for a new iPhone, provided certain conditions are met. One of the conditions of this program requires the customer to finance the initial purchase price of the iPhone with a third-party lender. Upon exercise of the trade-in right and purchase of a new iPhone, the Company satisfies the customer’s outstanding balance due to the third-party lender on the original device. The Company accounts for the trade-in right as a guarantee liability and recognizes arrangement revenue net of the fair value of such right with subsequent changes to the guarantee liability recognized within revenue.

The Company has entered into indemnification agreements with its directors and executive officers. Under these agreements, the Company has agreed to indemnify such individuals to the fullest extent permitted by law against liabilities that arise by reason of their status as directors or officers and to advance expenses incurred by such individuals in connection with related legal proceedings. It is not possible to determine the maximum potential amount of payments the Company could be required to make under these agreements due to the limited history of prior indemnification claims and the unique facts and circumstances involved in each claim. However, the Company maintains directors and officers liability insurance coverage to reduce its exposure to such obligations.

Concentrations in the Available Sources of Supply of Materials and Product

Although most components essential to the Company’s business are generally available from multiple sources, a number of components are currently obtained from single or limited sources. In addition, the Company competes for various components with other participants in the markets for mobile communication and media devices and personal computers. Therefore, many components used by the Company, including those that are available from multiple sources, are at times subject to industry-wide shortage and significant pricing fluctuations that could materially adversely affect the Company’s financial condition and operating results.

The Company uses some custom components that are not commonly used by its competitors, and new products introduced by the Company often utilize custom components available from only one source. When a component or product uses new technologies, initial capacity constraints may exist until the suppliers' yields have matured or manufacturing capacity has increased. If the Company's supply of components for a new or existing product were delayed or constrained, or if an outsourcing partner delayed shipments of completed products to the Company, the Company's financial condition and operating results could be materially adversely affected. The Company's business and financial performance could also be materially adversely affected depending on the time required to obtain sufficient quantities from the original source, or to identify and obtain sufficient quantities from an alternative source. Continued availability of these components at acceptable prices, or at all, may be affected if those suppliers concentrated on the production of common components instead of components customized to meet the Company's requirements.

The Company has entered into agreements for the supply of many components; however, there can be no guarantee that the Company will be able to extend or renew these agreements on similar terms, or at all. Therefore, the Company remains subject to significant risks of supply shortages and price increases that could materially adversely affect its financial condition and operating results.

Substantially all of the Company's hardware products are manufactured by outsourcing partners that are located primarily in Asia. A significant concentration of this manufacturing is currently performed by a small number of outsourcing partners, often in single locations. Certain of these outsourcing partners are the sole-sourced suppliers of components and manufacturers for many of the Company's products. Although the Company works closely with its outsourcing partners on manufacturing schedules, the Company's operating results could be adversely affected if its outsourcing partners were unable to meet their production commitments. The Company's purchase commitments typically cover its requirements for periods up to 150 days.

Other Off-Balance Sheet Commitments

Operating Leases

The Company leases various equipment and facilities, including retail space, under noncancelable operating lease arrangements. The Company does not currently utilize any other off-balance sheet financing arrangements. The major facility leases are typically for terms not exceeding 10 years and generally contain multi-year renewal options. As of September 26, 2015, the Company had a total of 463 retail stores. Leases for retail space are for terms ranging from five to 20 years, the majority of which are for 10 years, and often contain multi-year renewal options. As of September 26, 2015, the Company's total future minimum lease payments under noncancelable operating leases were $6.3 billion, of which $3.6 billion related to leases for retail space.

Rent expense under all operating leases, including both cancelable and noncancelable leases, was $794 million, $717 million and $645 million in 2015, 2014 and 2013, respectively. Future minimum lease payments under noncancelable operating leases having remaining terms in excess of one year as of September 26, 2015, are as follows (in millions):

2016	$ 772
2017	774
2018	744
2019	715
2020	674
Thereafter	2,592
Total	$ 6,271

Other Commitments

The Company utilizes several outsourcing partners to manufacture sub-assemblies for the Company's products and to perform final assembly and testing of finished products. These outsourcing partners acquire components and build product based on demand information supplied by the Company, which typically covers periods up to 150 days. The Company also obtains individual components for its products from a wide variety of individual suppliers. Consistent with industry practice, the Company acquires components through a combination of purchase orders, supplier contracts and open orders based on projected demand information. Where appropriate, the purchases are applied to inventory component prepayments that are outstanding with the respective supplier. As of September 26, 2015, the Company had outstanding off-balance sheet third-party manufacturing commitments and component purchase commitments of $29.5 billion.

In addition to the commitments mentioned above, the Company had other off-balance sheet obligations of $7.3 billion as of September 26, 2015 that consisted of commitments to acquire capital assets, including product tooling and manufacturing process equipment, and commitments related to inventory prepayments, advertising, licensing, R&D, internet and telecommunications services, energy and other obligations.

Contingencies

The Company is subject to various legal proceedings and claims that have arisen in the ordinary course of business and that have not been fully adjudicated, certain of which are discussed in Part I, Item 1A of this Form 10-K under the heading “Risk Factors” and in Part I, Item 3 of this Form 10-K under the heading “Legal Proceedings.” In the opinion of management, there was not at least a reasonable possibility the Company may have incurred a material loss, or a material loss in excess of a recorded accrual, with respect to loss contingencies for asserted legal and other claims. However, the outcome of litigation is inherently uncertain. Therefore, although management considers the likelihood of such an outcome to be remote, if one or more of these legal matters were resolved against the Company in a reporting period for amounts in excess of management’s expectations, the Company’s consolidated financial statements for that reporting period could be materially adversely affected.

Apple Inc. v. Samsung Electronics Co., Ltd, et al.

On August 24, 2012, a jury returned a verdict awarding the Company $1.05 billion in its lawsuit against Samsung Electronics Co., Ltd and affiliated parties in the United States District Court, Northern District of California, San Jose Division. On March 6, 2014, the District Court entered final judgment in favor of the Company in the amount of approximately $930 million. On May 18, 2015, the U.S. Court of Appeals for the Federal Circuit affirmed in part, and reversed in part, the decision of the District Court. As a result, the Court of Appeals ordered entry of final judgment on damages in the amount of approximately $548 million, with the District Court to determine supplemental damages and interest, as well as damages owed for products subject to the reversal in part. Because the ruling remains subject to further proceedings, the Company has not recognized the award in its results of operations.

Note 11 – Segment Information and Geographic Data

The Company reports segment information based on the “management” approach. The management approach designates the internal reporting used by management for making decisions and assessing performance as the source of the Company’s reportable operating segments.

The Company manages its business primarily on a geographic basis. The Company’s reportable operating segments consist of the Americas, Europe, Greater China, Japan and Rest of Asia Pacific. The Americas segment includes both North and South America. The Europe segment includes European countries, as well as India, the Middle East and Africa. The Greater China segment includes China, Hong Kong and Taiwan. The Rest of Asia Pacific segment includes Australia and those Asian countries not included in the Company’s other reportable operating segments. Although each reportable operating segment provides similar hardware and software products and similar services, they are managed separately to better align with the location of the Company’s customers and distribution partners and the unique market dynamics of each geographic region. The accounting policies of the various segments are the same as those described in Note 1, “Summary of Significant Accounting Policies.”

The Company evaluates the performance of its reportable operating segments based on net sales and operating income. Net sales for geographic segments are generally based on the location of customers and sales through the Company’s retail stores located in those geographic locations. Operating income for each segment includes net sales to third parties, related cost of sales and operating expenses directly attributable to the segment. Advertising expenses are generally included in the geographic segment in which the expenditures are incurred. Operating income for each segment excludes other income and expense and certain expenses managed outside the reportable operating segments. Costs excluded from segment operating income include various corporate expenses such as R&D, corporate marketing expenses, certain share-based compensation expenses, income taxes, various nonrecurring charges and other separately managed general and administrative costs. The Company does not include intercompany transfers between segments for management reporting purposes.

The following table shows information by reportable operating segment for 2015, 2014 and 2013 (in millions):

	2015	2014	2013
Americas:			
Net sales	$ 93,864	$ 80,095	$ 77,093
Operating income	$ 31,186	$ 26,158	$ 24,829
Europe:			
Net sales	$ 50,337	$ 44,285	$ 40,980
Operating income	$ 16,527	$ 14,434	$ 12,767
Greater China:			
Net sales	$ 58,715	$ 31,853	$ 27,016
Operating income	$ 23,002	$ 11,039	$ 8,499
Japan:			
Net sales	$ 15,706	$ 15,314	$ 13,782
Operating income	$ 7,617	$ 6,904	$ 6,668
Rest of Asia Pacific:			
Net sales	$ 15,093	$ 11,248	$ 12,039
Operating income	$ 5,518	$ 3,674	$ 3,762

A reconciliation of the Company's segment operating income to the Consolidated Statements of Operations for 2015, 2014 and 2013 is as follows (in millions):

	2015	2014	2013
Segment operating income	$ 83,850	$ 62,209	$ 56,525
Research and development expense	(8,067)	(6,041)	(4,475)
Other corporate expenses, net	(4,553)	(3,665)	(3,051)
Total operating income	$ 71,230	$ 52,503	$ 48,999

The U.S. and China were the only countries that accounted for more than 10% of the Company's net sales in 2015, 2014 and 2013. There was no single customer that accounted for more than 10% of net sales in 2015, 2014 or 2013. Net sales for 2015, 2014 and 2013 and long-lived assets as of September 26, 2015 and September 27, 2014 are as follows (in millions):

	2015	2014	2013
Net sales:			
U.S.	$ 81,732	$ 68,909	$ 66,197
China [(1)]	56,547	30,638	25,946
Other countries	95,436	83,248	78,767
Total net sales	$ 233,715	$ 182,795	$ 170,910

	2015	2014
Long-lived assets:		
U.S.	$ 12,022	$ 9,108
China [(1)]	8,722	9,477
Other countries	3,040	2,917
Total long-lived assets	$ 23,784	$ 21,502

[(1)] China includes Hong Kong. Long-lived assets located in China consist primarily of product tooling and manufacturing process equipment and assets related to retail stores and related infrastructure.

Net sales by product for 2015, 2014 and 2013 are as follows (in millions):

	2015	2014	2013
Net Sales by Product:			
iPhone [1]	$ 155,041	$ 101,991	$ 91,279
iPad [1]	23,227	30,283	31,980
Mac [1]	25,471	24,079	21,483
Services [2]	19,909	18,063	16,051
Other Products [1][3]	10,067	8,379	10,117
Total net sales	$ 233,715	$ 182,795	$ 170,910

[1] Includes deferrals and amortization of related software upgrade rights and non-software services.

[2] Includes revenue from the iTunes Store, App Store, Mac App Store, iBooks Store, Apple Music, AppleCare, Apple Pay, licensing and other services.

[3] Includes sales of Apple TV, Apple Watch, Beats products, iPod and Apple-branded and third-party accessories.

Note 12 – Selected Quarterly Financial Information (Unaudited)

The following tables show a summary of the Company’s quarterly financial information for each of the four quarters of 2015 and 2014 (in millions, except per share amounts):

	Fourth Quarter	Third Quarter	Second Quarter	First Quarter
2015:				
Net sales	$ 51,501	$ 49,605	$ 58,010	$ 74,599
Gross margin	$ 20,548	$ 19,681	$ 23,656	$ 29,741
Net income	$ 11,124	$ 10,677	$ 13,569	$ 18,024
Earnings per share [1]:				
Basic	$ 1.97	$ 1.86	$ 2.34	$ 3.08
Diluted	$ 1.96	$ 1.85	$ 2.33	$ 3.06

	Fourth Quarter	Third Quarter	Second Quarter	First Quarter
2014:				
Net sales	$ 42,123	$ 37,432	$ 45,646	$ 57,594
Gross margin	$ 16,009	$ 14,735	$ 17,947	$ 21,846
Net income	$ 8,467	$ 7,748	$ 10,223	$ 13,072
Earnings per share [1]:				
Basic	$ 1.43	$ 1.29	$ 1.67	$ 2.08
Diluted	$ 1.42	$ 1.28	$ 1.66	$ 2.07

[1] Basic and diluted earnings per share are computed independently for each of the quarters presented. Therefore, the sum of quarterly basic and diluted per share information may not equal annual basic and diluted earnings per share.

Report of Ernst & Young LLP, Independent Registered Public Accounting Firm

The Board of Directors and Shareholders of Apple Inc.

We have audited the accompanying consolidated balance sheets of Apple Inc. as of September 26, 2015 and September 27, 2014, and the related consolidated statements of operations, comprehensive income, shareholders' equity and cash flows for each of the three years in the period ended September 26, 2015. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the consolidated financial position of Apple Inc. at September 26, 2015 and September 27, 2014, and the consolidated results of its operations and its cash flows for each of the three years in the period ended September 26, 2015, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), Apple Inc.'s internal control over financial reporting as of September 26, 2015, based on criteria established in *Internal Control – Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) and our report dated October 28, 2015 expressed an unqualified opinion thereon.

/s/ Ernst & Young LLP

San Jose, California
October 28, 2015

Report of Ernst & Young LLP, Independent Registered Public Accounting Firm

The Board of Directors and Shareholders of Apple Inc.

We have audited Apple Inc.'s internal control over financial reporting as of September 26, 2015, based on criteria established in *Internal Control – Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) ("the COSO criteria"). Apple Inc.'s management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Management's Annual Report on Internal Control Over Financial Reporting. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, Apple Inc. maintained, in all material respects, effective internal control over financial reporting as of September 26, 2015, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the 2015 consolidated financial statements of Apple Inc. and our report dated October 28, 2015 expressed an unqualified opinion thereon.

/s/ Ernst & Young LLP

San Jose, California
October 28, 2015

Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure

None.

Item 9A. Controls and Procedures

Evaluation of Disclosure Controls and Procedures

Based on an evaluation under the supervision and with the participation of the Company's management, the Company's principal executive officer and principal financial officer have concluded that the Company's disclosure controls and procedures as defined in Rules 13a-15(e) and 15d-15(e) under the Securities Exchange Act of 1934, as amended (the "Exchange Act") were effective as of September 26, 2015 to provide reasonable assurance that information required to be disclosed by the Company in reports that it files or submits under the Exchange Act is (i) recorded, processed, summarized and reported within the time periods specified in the Securities and Exchange Commission rules and forms and (ii) accumulated and communicated to the Company's management, including its principal executive officer and principal financial officer, as appropriate to allow timely decisions regarding required disclosure.

Inherent Limitations Over Internal Controls

The Company's internal control over financial reporting is designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with U.S. generally accepted accounting principles ("GAAP"). The Company's internal control over financial reporting includes those policies and procedures that:

(i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the Company's assets;

(ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that the Company's receipts and expenditures are being made only in accordance with authorizations of the Company's management and directors; and

(iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the Company's assets that could have a material effect on the financial statements.

Management, including the Company's Chief Executive Officer and Chief Financial Officer, does not expect that the Company's internal controls will prevent or detect all errors and all fraud. A control system, no matter how well designed and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system are met. Further, the design of a control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs. Because of the inherent limitations in all control systems, no evaluation of internal controls can provide absolute assurance that all control issues and instances of fraud, if any, have been detected. Also, any evaluation of the effectiveness of controls in future periods are subject to the risk that those internal controls may become inadequate because of changes in business conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Management's Annual Report on Internal Control Over Financial Reporting

The Company's management is responsible for establishing and maintaining adequate internal control over financial reporting (as defined in Rule 13a-15(f) under the Exchange Act). Management conducted an assessment of the effectiveness of the Company's internal control over financial reporting based on the criteria set forth in Internal Control – Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework). Based on the Company's assessment, management has concluded that its internal control over financial reporting was effective as of September 26, 2015 to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with GAAP. The Company's independent registered public accounting firm, Ernst & Young LLP, has issued an audit report on the Company's internal control over financial reporting, which appears in Part II, Item 8 of this Form 10-K.

Changes in Internal Control Over Financial Reporting

There were no changes in the Company's internal control over financial reporting during the fourth quarter of 2015, which were identified in connection with management's evaluation required by paragraph (d) of rules 13a-15 and 15d-15 under the Exchange Act, that have materially affected, or are reasonably likely to materially affect, the Company's internal control over financial reporting.

Item 9B. Other Information

Not applicable.

PART III

Item 10. Directors, Executive Officers and Corporate Governance

The information required by this Item is set forth under the headings “Directors, Corporate Governance and Executive Officers” in the Company’s 2016 Proxy Statement to be filed with the U.S. Securities and Exchange Commission (the “SEC”) within 120 days after September 26, 2015 in connection with the solicitation of proxies for the Company’s 2016 annual meeting of shareholders and is incorporated herein by reference.

The Company has a code of ethics, “Business Conduct: The way we do business worldwide,” that applies to all employees, including the Company’s principal executive officer, principal financial officer, and principal accounting officer, as well as to the members of the Board of Directors of the Company. The code is available at investor.apple.com/corporate-governance.cfm. The Company intends to disclose any changes in, or waivers from, this code by posting such information on the same website or by filing a Form 8-K, in each case to the extent such disclosure is required by rules of the SEC or the NASDAQ Stock Market LLC.

Item 11. Executive Compensation

The information required by this Item is set forth under the heading “Executive Compensation” and under the subheadings “Board Oversight of Risk Management,” “Compensation Committee Interlocks and Insider Participation,” “Compensation of Directors” and “Director Compensation-2015” under the heading “Directors, Corporate Governance and Executive Officers” in the Company’s 2016 Proxy Statement to be filed with the SEC within 120 days after September 26, 2015 and is incorporated herein by reference.

Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters

The information required by this Item is set forth under the headings “Security Ownership of Certain Beneficial Owners and Management” and “Equity Compensation Plan Information” in the Company’s 2016 Proxy Statement to be filed with the SEC within 120 days after September 26, 2015 and is incorporated herein by reference.

Item 13. Certain Relationships and Related Transactions, and Director Independence

The information required by this Item is set forth under the subheadings “Board Committees”, “Review, Approval or Ratification of Transactions with Related Persons” and “Transactions with Related Persons” under the heading “Directors, Corporate Governance and Executive Officers” in the Company’s 2016 Proxy Statement to be filed with the SEC within 120 days after September 26, 2015 and is incorporated herein by reference.

Item 14. Principal Accounting Fees and Services

The information required by this Item is set forth under the subheadings “Fees Paid to Auditors” and “Policy on Audit Committee Pre-Approval of Audit and Non-Audit Services Performed by the Independent Registered Public Accounting Firm” under the proposal “Ratification of Appointment of Independent Registered Public Accounting Firm” in the Company’s 2016 Proxy Statement to be filed with the SEC within 120 days after September 26, 2015 and is incorporated herein by reference.

PART IV

Item 15. Exhibits, Financial Statement Schedules

(a) Documents filed as part of this report

(1) All financial statements

(2) Financial Statement Schedules

All financial statement schedules have been omitted, since the required information is not applicable or is not present in amounts sufficient to require submission of the schedule, or because the information required is included in the consolidated financial statements and notes thereto included in this Form 10-K.

(3) Exhibits required by Item 601 of Regulation S-K

The information required by this Section (a)(3) of Item 15 is set forth on the exhibit index that follows the Signatures page of this Form 10-K.

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, the Registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

Date: October 28, 2015

Apple Inc.

By: /s/ Luca Maestri

Luca Maestri
Senior Vice President,
Chief Financial Officer

Power of Attorney

KNOW ALL PERSONS BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints Timothy D. Cook and Luca Maestri, jointly and severally, his or her attorneys-in-fact, each with the power of substitution, for him or her in any and all capacities, to sign any amendments to this Annual Report on Form 10-K, and to file the same, with exhibits thereto and other documents in connection therewith, with the Securities and Exchange Commission, hereby ratifying and confirming all that each of said attorneys-in-fact, or his substitute or substitutes, may do or cause to be done by virtue hereof.

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the Registrant and in the capacities and on the dates indicated:

Name	Title	Date
/s/ Timothy D. Cook TIMOTHY D. COOK	Chief Executive Officer and Director (Principal Executive Officer)	October 28, 2015
/s/ Luca Maestri LUCA MAESTRI	Senior Vice President, Chief Financial Officer (Principal Financial Officer)	October 28, 2015
/s/ Chris Kondo CHRIS KONDO	Senior Director of Corporate Accounting (Principal Accounting Officer)	October 28, 2015
/s/ Al Gore AL GORE	Director	October 28, 2015
/s/ Robert A. Iger ROBERT A. IGER	Director	October 28, 2015
/s/ Andrea Jung ANDREA JUNG	Director	October 28, 2015
/s/ Arthur D. Levinson ARTHUR D. LEVINSON	Director	October 28, 2015
/s/ Ronald D. Sugar RONALD D. SUGAR	Director	October 28, 2015
/s/ Susan L. Wagner SUSAN L. WAGNER	Director	October 28, 2015

EXHIBIT INDEX [(1)]

Exhibit Number	Exhibit Description	Incorporated by Reference		
		Form	Exhibit	Filing Date/ Period End Date
3.1	Restated Articles of Incorporation of the Registrant effective as of June 6, 2014.	8-K	3.1	6/6/14
3.2	Amended and Restated Bylaws of the Registrant effective as of February 28, 2014.	8-K	3.2	3/5/14
4.1	Form of Common Stock Certificate of the Registrant.	10-Q	4.1	12/30/06
4.2	Indenture, dated as of April 29, 2013, between the Registrant and The Bank of New York Mellon Trust Company, N.A., as Trustee.	S-3	4.1	4/29/13
4.3	Officer's Certificate of the Registrant, dated as of May 3, 2013, including forms of global notes representing the Floating Rate Notes due 2016, Floating Rate Notes due 2018, 0.45% Notes due 2016, 1.00% Notes due 2018, 2.40% Notes due 2023 and 3.85% Notes due 2043.	8-K	4.1	5/3/13
4.4	Officer's Certificate of the Registrant, dated as of May 6, 2014, including forms of global notes representing the Floating Rate Notes due 2017, Floating Rate Notes due 2019, 1.05% Notes due 2017, 2.10% Notes due 2019, 2.85% Notes due 2021, 3.45% Notes due 2024 and 4.45% Notes due 2044.	8-K	4.1	5/6/14
4.5	Officer's Certificate of the Registrant, dated as of November 10, 2014, including forms of global notes representing the 1.000% Notes due 2022 and 1.625% Notes due 2026.	8-K	4.1	11/10/14
4.6	Officer's Certificate of the Registrant, dated as of February 9, 2015, including forms of global notes representing the Floating Rate Notes due 2020, 1.55% Notes due 2020, 2.15% Notes due 2022, 2.50% Notes due 2025 and 3.45% Notes due 2045.	8-K	4.1	2/9/15
4.7	Officer's Certificate of the Registrant, dated as of May 13, 2015, including forms of global notes representing the Floating Rate Notes due 2017, Floating Rate Notes due 2020, 0.900% Notes due 2017, 2.000% Notes due 2020, 2.700% Notes due 2022, 3.200% Notes due 2025, and 4.375% Notes due 2045.	8-K	4.1	5/13/15
4.8	Officer's Certificate of the Registrant, dated as of June 10, 2015, including forms of global notes representing the 0.35% Notes due 2020.	8-K	4.1	6/10/15
4.9	Officer's Certificate of the Registrant, dated as of July 31, 2015, including forms of global notes representing the 3.05% Notes due 2029 and 3.60% Notes due 2042.	8-K	4.1	7/31/15
4.10	Officer's Certificate of the Registrant, dated as of September 17, 2015, including forms of global notes representing the 1.375% Notes due 2024 and 2.000% Notes due 2027.	8-K	4.1	9/17/15
10.1*	Employee Stock Purchase Plan, as amended and restated as of March 10, 2015.	8-K	10.1	3/13/15
10.2*	Form of Indemnification Agreement between the Registrant and each director and executive officer of the Registrant.	10-Q	10.2	6/27/09
10.3*	1997 Director Stock Plan, as amended through August 23, 2012.	10-Q	10.3	12/28/13
10.4*	2003 Employee Stock Plan, as amended through February 25, 2010.	8-K	10.1	3/1/10
10.5*	Form of Restricted Stock Unit Award Agreement under 2003 Employee Stock Plan effective as of November 16, 2010.	10-Q	10.10	12/25/10
10.6*	Form of Restricted Stock Unit Award Agreement under 2003 Employee Stock Plan effective as of April 6, 2012.	10-Q	10.8	3/31/12

Exhibit Number	Exhibit Description	Incorporated by Reference Form	 Exhibit	 Filing Date/ Period End Date
10.7*	Summary Description of Amendment, effective as of May 24, 2012, to certain Restricted Stock Unit Award Agreements outstanding as of April 5, 2012.	10-Q	10.8	6/30/12
10.8*	2014 Employee Stock Plan.	8-K	10.1	3/5/14
10.9*	Form of Restricted Stock Unit Award Agreement under 2014 Employee Stock Plan as of February 28, 2014.	8-K	10.2	3/5/14
10.10*	Form of Performance Award Agreement under 2014 Employee Stock Plan effective as of February 28, 2014.	8-K	10.3	3/5/14
10.11*	Form of Restricted Stock Unit Award Agreement under 2014 Employee Stock Plan effective as of August 26, 2014.	10-K	10.11	9/27/14
10.12*	Form of Performance Award Agreement under 2014 Employee Stock Plan effective as of August 26, 2014.	10-K	10.12	9/27/14
10.13*	Form of Amendment, effective as of August 26, 2014, to Restricted Stock Unit Award Agreements and Performance Award Agreements outstanding as of August 26, 2014.	10-K	10.13	9/27/14
10.14*	Offer Letter, dated August 1, 2013, from the Registrant to Angela Ahrendts.	10-Q	10.14	12/27/14
12.1**	Computation of Ratio of Earnings to Fixed Charges.			
21.1**	Subsidiaries of the Registrant.			
23.1**	Consent of Ernst & Young LLP, Independent Registered Public Accounting Firm.			
24.1**	Power of Attorney (included on the Signatures page of this Annual Report on Form 10-K).			
31.1**	Rule 13a-14(a) / 15d-14(a) Certification of Chief Executive Officer.			
31.2**	Rule 13a-14(a) / 15d-14(a) Certification of Chief Financial Officer.			
32.1***	Section 1350 Certifications of Chief Executive Officer and Chief Financial Officer.			
101.INS**	XBRL Instance Document.			
101.SCH**	XBRL Taxonomy Extension Schema Document.			
101.CAL**	XBRL Taxonomy Extension Calculation Linkbase Document.			
101.DEF**	XBRL Taxonomy Extension Definition Linkbase Document.			
101.LAB**	XBRL Taxonomy Extension Label Linkbase Document.			
101.PRE**	XBRL Taxonomy Extension Presentation Linkbase Document.			

* Indicates management contract or compensatory plan or arrangement.

** Filed herewith.

*** Furnished herewith.

[1] Certain instruments defining the rights of holders of long-term debt securities of the Registrant are omitted pursuant to Item 601(b)(4)(iii) of Regulation S-K. The Registrant hereby undertakes to furnish to the SEC, upon request, copies of any such instruments.

Exhibit 12.1

Apple Inc.
Computation of Ratio of Earnings to Fixed Charges
(In millions, except ratios)

	Years ended				
	September 26, 2015	September 27, 2014	September 28, 2013	September 29, 2012	September 24, 2011
Earnings:					
Earnings before provision for income taxes	$ 72,515	$ 53,483	$ 50,155	$ 55,763	$ 34,205
Add: Fixed Charges	892	527	265	98	68
Total Earnings	$ 73,407	$ 54,010	$ 50,420	$ 55,861	$ 34,273
Fixed Charges [1]:					
Interest Expense	$ 733	$ 384	$ 136	$ 0	$ 0
Interest component of rental expense	159	143	129	98	68
Total Fixed Charges	$ 892	$ 527	$ 265	$ 98	$ 68
Ratio of Earnings to Fixed Charges [2]	82	102	190	570	504

[1] Fixed charges include the portion of rental expense that management believes is representative of the interest component.

[2] The ratio of earnings to fixed charges is computed by dividing Total Earnings by Total Fixed Charges.

Exhibit 21.1

Subsidiaries of
Apple Inc.*

	Jurisdiction of Incorporation
Apple Sales International	Ireland
Apple Operations International	Ireland
Apple Operations Europe	Ireland
Braeburn Capital, Inc.	Nevada, U.S.

* Pursuant to Item 601(b)(21)(ii) of Regulation S-K, the names of other subsidiaries of Apple Inc. are omitted because, considered in the aggregate, they would not constitute a significant subsidiary as of the end of the year covered by this report.

Exhibit 23.1

Consent of Ernst & Young LLP, Independent Registered Public Accounting Firm

We consent to the incorporation by reference in the following Registration Statements:

(1) Registration Statement (Form S-8 No. 333-203698) pertaining to Apple Inc. Employee Stock Purchase Plan,

(2) Registration Statement (Form S-8 No. 333-195509) pertaining to Apple Inc. 2014 Employee Stock Plan,

(3) Registration Statement (Form S-8 No. 333-193709) pertaining to Topsy Labs, Inc. 2007 Stock Plan,

(4) Registration Statement (Form S-3 ASR No. 333-188191) of Apple Inc.,

(5) Registration Statement (Form S-8 No. 333-184706) pertaining to AuthenTec, Inc. 2007 Stock Incentive Plan and AuthenTec, Inc. 2010 Incentive Plan, as amended,

(6) Registration Statement (Form S-8 No. 333-180981) pertaining to Chomp Inc. 2009 Equity Incentive Plan,

(7) Registration Statement (Form S-8 No. 333-179189) pertaining to Anobit Technologies Ltd. Global Share Incentive Plan (2006),

(8) Registration Statement (Form S-8 No. 333-168279) pertaining to Siri, Inc. 2008 Stock Option/Stock Issuance Plan,

(9) Registration Statement (Form S-8 No. 333-165214) pertaining to Apple Inc. 2003 Employee Stock Plan, la la media, inc. 2005 Stock Plan and Quattro Wireless, Inc. 2006 Stock Option and Grant Plan,

(10) Registration Statement (Form S-8 No. 333-146026) pertaining to Apple Inc. 2003 Employee Stock Plan and Apple Inc. Amended Employee Stock Purchase Plan,

(11) Registration Statement (Form S-8 No. 333-125148) pertaining to Employee Stock Purchase Plan and 2003 Employee Stock Plan, and

(12) Registration Statement (Form S-8 No. 333-60455) pertaining to 1997 Director Stock Option Plan;

of our reports dated October 28, 2015 with respect to the consolidated financial statements of Apple Inc., and the effectiveness of internal control over financial reporting of Apple Inc., included in this Annual Report on Form 10-K for the year ended September 26, 2015.

/s/ Ernst & Young LLP

San Jose, California
October 28, 2015

Exhibit 31.1

CERTIFICATION

I, Timothy D. Cook, certify that:

1. I have reviewed this annual report on Form 10-K of Apple Inc.;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the Registrant as of, and for, the periods presented in this report;

4. The Registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the Registrant and have:

   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the Registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   (c) Evaluated the effectiveness of the Registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   (d) Disclosed in this report any change in the Registrant's internal control over financial reporting that occurred during the Registrant's most recent fiscal quarter (the Registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the Registrant's internal control over financial reporting; and

5. The Registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the Registrant's auditors and the audit committee of the Registrant's board of directors (or persons performing the equivalent functions):

   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the Registrant's ability to record, process, summarize, and report financial information; and

   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the Registrant's internal control over financial reporting.

Date: October 28, 2015

By: /s/ Timothy D. Cook
Timothy D. Cook
Chief Executive Officer

Exhibit 31.2

CERTIFICATION

I, Luca Maestri, certify that:

1. I have reviewed this annual report on Form 10-K of Apple Inc.;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the Registrant as of, and for, the periods presented in this report;

4. The Registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the Registrant and have:

   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the Registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   (c) Evaluated the effectiveness of the Registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   (d) Disclosed in this report any change in the Registrant's internal control over financial reporting that occurred during the Registrant's most recent fiscal quarter (the Registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the Registrant's internal control over financial reporting; and

5. The Registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the Registrant's auditors and the audit committee of the Registrant's board of directors (or persons performing the equivalent functions):

   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the Registrant's ability to record, process, summarize, and report financial information; and

   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the Registrant's internal control over financial reporting.

Date: October 28, 2015

By: /s/ Luca Maestri

Luca Maestri
Senior Vice President,
Chief Financial Officer

Exhibit 32.1

CERTIFICATIONS OF CHIEF EXECUTIVE OFFICER AND CHIEF FINANCIAL OFFICER PURSUANT TO 18 U.S.C. SECTION 1350, AS ADOPTED PURSUANT TO SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002

I, Timothy D. Cook, certify, as of the date hereof, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that the Annual Report of Apple Inc. on Form 10-K for the fiscal year ended September 26, 2015 fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934 and that information contained in such Form 10-K fairly presents in all material respects the financial condition and results of operations of Apple Inc. at the dates and for the periods indicated.

Date: October 28, 2015

By: /s/ Timothy D. Cook
Timothy D. Cook
Chief Executive Officer

I, Luca Maestri, certify, as of the date hereof, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that the Annual Report of Apple Inc. on Form 10-K for the fiscal year ended September 26, 2015 fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934 and that information contained in such Form 10-K fairly presents in all material respects the financial condition and results of operations of Apple Inc. at the dates and for the periods indicated.

Date: October 28, 2015

By: /s/ Luca Maestri
Luca Maestri
Senior Vice President,
Chief Financial Officer

A signed original of this written statement required by Section 906 has been provided to Apple Inc. and will be retained by Apple Inc. and furnished to the Securities and Exchange Commission or its staff upon request.

Exhibit 3

ENGLISH

IMPORTANT: BY USING YOUR iPHONE, iPAD OR iPOD TOUCH ("iOS DEVICE"), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS:

A. APPLE iOS SOFTWARE LICENSE AGREEMENT
B. APPLE PAY SUPPLEMENTAL TERMS
C. NOTICES FROM APPLE

APPLE INC.
iOS SOFTWARE LICENSE AGREEMENT
Single Use License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR iOS DEVICE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR iOS DEVICE OR DOWNLOADING A SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE iOS DEVICE OR DOWNLOAD THE SOFTWARE UPDATE.

IF YOU HAVE RECENTLY PURCHASED AN iOS DEVICE AND YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE iOS DEVICE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT http://www.apple.com/legal/sales_policies/.

1. General.
(a) The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with your iOS Device ("Original iOS Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("iOS Software Updates"), whether in read only memory, on any other media or in any other form (the Original iOS Software and iOS Software Updates are collectively referred to as the "iOS Software") are licensed, not sold, to you by Apple Inc. ("Apple") for use only under the terms of this License. Apple and its licensors retain ownership of the iOS Software itself and reserve all rights not expressly granted to you. You agree that the terms of this License will apply to any Apple-branded app that may be pre-installed on your iOS Device, unless such app is accompanied by a separate license, in which case you agree that the terms of that license will govern your use of that app.

(b) Apple, at its discretion, may make available future iOS Software Updates for your iOS Device. The iOS Software Updates, if any, may not necessarily include all existing software features or new features that Apple releases for newer or other models of iOS Devices. The terms of this License will govern any iOS Software Updates provided by Apple that replace and/or supplement the Original iOS Software product, unless such iOS Software Update is accompanied by a separate license in which case the terms of that license will govern.

2. Permitted License Uses and Restrictions.
(a) Subject to the terms and conditions of this License, you are granted a limited non-exclusive license to use the iOS Software on a single Apple-branded iOS Device. Except as permitted in Section 2(b) below, and unless as provided in a separate agreement between you and Apple, this License does not allow the iOS Software to exist on more than one Apple-branded iOS Device at a time, and you may not distribute or make the iOS Software available over a network where it could be used by multiple devices at the same time. This License does not grant you any rights to use Apple proprietary interfaces and other intellectual property in the design, development,

manufacture, licensing or distribution of third party devices and accessories, or third party software applications, for use with iOS Devices. Some of those rights are available under separate licenses from Apple. For more information on developing third party devices and accessories for iOS Devices, please visit https://developer.apple.com/programs/mfi/. For more information on developing software applications for iOS Devices, please visit https://developer.apple.com.

(b) Subject to the terms and conditions of this License, you are granted a limited non-exclusive license to download iOS Software Updates that may be made available by Apple for your model of the iOS Device to update or restore the software on any such iOS Device that you own or control. This License does not allow you to update or restore any iOS Device that you do not control or own, and you may not distribute or make the iOS Software Updates available over a network where they could be used by multiple devices or multiple computers at the same time. If you download an iOS Software Update to your computer, you may make one copy of the iOS Software Updates stored on your computer in machine-readable form for backup purposes only, provided that the backup copy must include all copyright or other proprietary notices contained on the original.

(c) To the extent that Apple has preinstalled Apple-branded apps from the App Store on your iOS Device at the time of purchase ("Preinstalled Apps"), you will need to log into the App Store and associate these Preinstalled Apps with your App Store account in order to use them on your iOS Device. When you associate a Preinstalled App with your App Store account, you will at the same time be automatically associating all other Preinstalled Apps on your iOS Device. By choosing to associate the Preinstalled Apps with your App Store account, you agree that Apple may transmit, collect, maintain, process and use both the Apple ID used by your App Store account and a unique hardware identifier collected from your iOS Device, as unique account identifiers for the purpose of verifying the eligibility of your request and providing you access to the Preinstalled Apps through the App Store. If you do not wish to use a Preinstalled App, you can delete it from your iOS Device at any time.

(d) You may not, and you agree not to or enable others to, copy (except as expressly permitted by this License), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of the iOS Software or any services provided by the iOS Software or any part thereof (except as and only to the extent any foregoing restriction is prohibited by applicable law or by licensing terms governing use of open-source components that may be included with the iOS Software).

(e) The iOS Software may be used to reproduce materials so long as such use is limited to reproduction of non-copyrighted materials, materials in which you own the copyright, or materials you are authorized or legally permitted to reproduce. Title and intellectual property rights in and to any content displayed by, stored on or accessed through your iOS Device belong to the respective content owner. Such content may be protected by copyright or other intellectual property laws and treaties, and may be subject to terms of use of the third party providing such content. Except as otherwise provided herein, this License does not grant you any rights to use such content nor does it guarantee that such content will continue to be available to you.

(f) You agree to use the iOS Software and the Services (as defined in Section 5 below) in compliance with all applicable laws, including local laws of the country or region in which you reside or in which you download or use the iOS Software and Services. Features of the iOS Software and the Services may not be available in all languages or regions, some features may vary by region, and some may be restricted or unavailable from your service provider. A Wi-Fi or cellular data connection is required for some features of the iOS Software and Services such as FaceTime or iMessage.

(g) Use of the App Store requires a unique user name and password combination, known as an Apple ID. An Apple ID is also required to access app updates and certain features of the iOS

Software and Services. In addition, you acknowledge that many features, built-in apps, and Services of the iOS Software transmit data and could impact charges to your data plan, and that you are responsible for any such charges. You can view and control which applications are permitted to use cellular data and view an estimate of how much data such applications have consumed under Cellular Data Settings. For more information, please consult the User Guide for your iOS Device.

(h) If you choose to allow automatic app updates, your iOS Device will periodically check with Apple for updates to the apps on your device and, if one is available, the update will automatically download and install onto your device. You can turn off the automatic app updates altogether at any time by going to Settings, tap iTunes & App Store, and under Automatic Downloads, turn off Updates.

(i) Using your iOS Device in some circumstances can distract you and may cause a dangerous situation (for example, avoid typing a text message while driving a car or using headphones while riding a bicycle). By using your iOS Device you agree that you are responsible for observing rules that prohibit or restrict the use of mobile phones or headphones (for example, the requirement to use hands-free options for making calls when driving).

3. Transfer. You may not rent, lease, lend, sell, redistribute, or sublicense the iOS Software. You may, however, make a one-time permanent transfer of all of your license rights to the iOS Software to another party in connection with the transfer of ownership of your iOS Device, provided that: (a) the transfer must include your iOS Device and all of the iOS Software, including all its component parts, original media, printed materials and this License; (b) you do not retain any copies of the iOS Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the iOS Software reads and agrees to accept the terms and conditions of this License.

4. Consent to Use of Data. When you use your device, your phone number and certain unique identifiers for your iOS Device are sent to Apple in order to allow others to reach you by your phone number when using various communication features of the iOS Software, such as iMessage and FaceTime. When you use iMessage, Apple may hold your messages in encrypted form for a limited period of time. You may turn off FaceTime or iMessage by going to the FaceTime or Messages settings on your iOS Device. Other iOS Software features may require information from your iOS Device. You can find more information on which features send information to Apple, what information they send and how it may be used, when you turn on or use these features, or by visiting http://www.apple.com/privacy/. At all times your information will be treated in accordance with Apple's Privacy Policy, which can be viewed at: http://www.apple.com/legal/privacy/.

5. Services and Third Party Materials.
(a) The iOS Software may enable access to Apple's iTunes Store, App Store, iBooks Store, Game Center, iCloud, Maps and other Apple and third party services and web sites (collectively and individually, "Services"). Such Services may not be available in all languages or in all countries. Use of these Services requires Internet access and use of certain Services may require an Apple ID, may require you to accept additional terms and may be subject to additional fees. By using this software in connection with an Apple ID, or other Apple Service, you agree to the applicable terms of service for that Service, such as the latest iTunes Store Terms and Conditions, latest iBooks Store Terms and Conditions for the country in which you access such Store(s) or Game Center Terms and Conditions, which you may access and review at http://www.apple.com/legal/internet-services/itunes/ww/, or the iCloud Terms and Conditions which can be found at http://www.apple.com/legal/internet-services/icloud/ww/, respectively.

(b) If you sign up for iCloud, certain iCloud features like "iCloud Photo Library", "My Photo Stream", "iCloud Photo Sharing", "Back Up" and "Find My iPhone" may be accessed directly from the iOS

Software. You acknowledge and agree that your use of iCloud and these features is subject to the latest terms and conditions of the iCloud service, which you may access and review at: http://www.apple.com/legal/internet-services/icloud/ww/.

(c) Maps. The maps service and features of the iOS Software ("Maps"), including map data coverage, may vary by region. When you use any location-based features within Maps, such as turn-by-turn navigation, traffic and local search, various location-related and usage information may be sent to Apple, including the real-time geographic location of your iOS Device, in order to process your request and help improve Maps. Such location and usage data is collected by Apple in a form that does not personally identify you. By using Maps, you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this information, to provide and improve the Maps features and service, and other Apple products and services. You may disable the location-based functionality of Maps by going to the Location Services setting on your iOS Device and turning off the individual location setting for Maps. Certain Maps features will however be unavailable if you disable the Location Services setting, such as turn-by-turn navigation.

(d) iBooks; Podcasts. If you choose to use the sync feature of the iBooks and Podcasts apps to synchronize your bookmarks, notes, collections and podcast subscription data across your iOS Devices and computers, you acknowledge that such data will be sent to Apple and stored in conjunction with the Apple ID you use for the iBooks Store or iTunes Store, in order to sync such data to your other devices and computers that are authorized to access content through that Apple ID. You can turn off syncing at any time by going to Settings and changing the syncing options for the iBooks and Podcasts apps, respectively.

(e) You understand that by using any of the Services, you may encounter content that may be deemed offensive, indecent, or objectionable, which content may or may not be identified as having explicit language, and that the results of any search or entering of a particular URL may automatically and unintentionally generate links or references to objectionable material. Nevertheless, you agree to use the Services at your sole risk and that Apple, its affiliates, agents, principals, or licensors shall have no liability to you for content that may be found to be offensive, indecent, or objectionable.

(f) Certain Services may display, include or make available content, data, information, applications or materials from third parties ("Third Party Materials") or provide links to certain third party web sites. By using the Services, you acknowledge and agree that Apple is not responsible for examining or evaluating the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect of such Third Party Materials or web sites. Apple, its officers, affiliates and subsidiaries do not warrant or endorse and do not assume and will not have any liability or responsibility to you or any other person for any third-party Services, Third Party Materials or web sites, or for any other materials, products, or services of third parties. Third Party Materials and links to other web sites are provided solely as a convenience to you.

(g) Neither Apple nor any of its content providers guarantees the availability, accuracy, completeness, reliability, or timeliness of stock information, location data or any other data displayed by any Services. Financial information displayed by any Services is for general informational purposes only and should not be relied upon as investment advice. Before executing any securities transaction based upon information obtained through the Services, you should consult with a financial or securities professional who is legally qualified to give financial or securities advice in your country or region. Location data provided by any Services, including the Apple Maps service, is provided for basic navigational and/or planning purposes only and is not intended to be relied upon in situations where precise location information is needed or where erroneous, inaccurate, time-delayed or incomplete location data may lead to death, personal injury, property or environmental damage. You agree that, the results you receive from the Maps service may vary from actual road or terrain conditions due to factors that can affect the accuracy of the Maps data, such as, but not limited to, weather, road and traffic conditions, and geopolitical events. For your safety when using the navigation feature, always pay attention to posted road signs and current road conditions. Follow safe driving practices and traffic regulations, and note that walking directions may not include sidewalks or pedestrian paths.

(h) To the extent that you upload any content through the use of the Services, you represent that you own all rights in, or have authorization or are otherwise legally permitted to upload, such content and that such content does not violate any terms of service applicable to the Services. You agree that the Services contain proprietary content, information and material that is owned by Apple, the site owner and/or their licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright. You agree that you will not use such proprietary content, information or materials other than for permitted use of the Services or in any manner that is inconsistent with the terms of this License or that infringes any intellectual property rights of a third party or Apple. No portion of the Services may be reproduced in any form or by any means. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the Services, in any manner, and you shall not exploit the Services in any unauthorized way whatsoever, including but not limited to, using the Services to transmit any computer viruses, worms, trojan horses or other malware, or by trespass or burdening network capacity. You further agree not to use the Services in any manner to harass, abuse, stalk, threaten, defame or otherwise infringe or violate the rights of any other party, and that Apple is not in any way responsible for any such use by you, nor for any harassing, threatening, defamatory, offensive, infringing or illegal messages or transmissions that you may receive as a result of using any of the Services.

(i) In addition, Services and Third Party Materials that may be accessed, linked to or displayed on the iOS Device are not available in all languages or in all countries or regions. Apple makes no representation that such Services and Third Party Materials are appropriate or available for use in any particular location. To the extent you choose to use or access such Services and Third Party Materials, you do so at your own initiative and are responsible for compliance with any applicable laws, including but not limited to applicable local laws and privacy and data collection laws. Sharing or syncing photos through your iOS Device may cause metadata, including photo location data, to be transmitted with the photos. Apple and its licensors reserve the right to change, suspend, remove, or disable access to any Services at any time without notice. In no event will Apple be liable for the removal of or disabling of access to any such Services. Apple may also impose limits on the use of or access to certain Services, in any case and without notice or liability.

6. Termination. This License is effective until terminated. Your rights under this License will terminate automatically or otherwise cease to be effective without notice from Apple if you fail to comply with any term(s) of this License. Upon the termination of this License, you shall cease all use of the iOS Software. Sections 4, 5, 6, 7, 8, 9, 12 and 13 of this License shall survive any such termination.

7. Disclaimer of Warranties.
7.1 If you are a customer who is a consumer (someone who uses the iOS Software outside of your trade, business or profession), you may have legal rights in your country of residence which would prohibit the following limitations from applying to you, and where prohibited they will not apply to you. To find out more about rights, you should contact a local consumer advice organization.

7.2 YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, USE OF THE iOS SOFTWARE AND ANY SERVICES PERFORMED BY OR ACCESSED THROUGH THE iOS SOFTWARE IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK

AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU.

7.3 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE iOS SOFTWARE AND SERVICES ARE PROVIDED “AS IS” AND “AS AVAILABLE”, WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND APPLE AND APPLE’S LICENSORS (COLLECTIVELY REFERRED TO AS “APPLE” FOR THE PURPOSES OF SECTIONS 7 AND 8) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE iOS SOFTWARE AND SERVICES, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, QUIET ENJOYMENT, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

7.4 APPLE DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE iOS SOFTWARE AND SERVICES, THAT THE FUNCTIONS CONTAINED IN, OR SERVICES PERFORMED OR PROVIDED BY, THE iOS SOFTWARE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE iOS SOFTWARE AND SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, THAT ANY SERVICE WILL CONTINUE TO BE MADE AVAILABLE, THAT DEFECTS IN THE iOS SOFTWARE OR SERVICES WILL BE CORRECTED, OR THAT THE iOS SOFTWARE WILL BE COMPATIBLE OR WORK WITH ANY THIRD PARTY SOFTWARE, APPLICATIONS OR THIRD PARTY SERVICES. INSTALLATION OF THIS iOS SOFTWARE MAY AFFECT THE AVAILABILITY AND USABILITY OF THIRD PARTY SOFTWARE, APPLICATIONS OR THIRD PARTY SERVICES, AS WELL AS APPLE PRODUCTS AND SERVICES.

7.5 YOU FURTHER ACKNOWLEDGE THAT THE iOS SOFTWARE AND SERVICES ARE NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN, THE CONTENT, DATA OR INFORMATION PROVIDED BY THE iOS SOFTWARE OR SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE, INCLUDING WITHOUT LIMITATION THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT OR WEAPONS SYSTEMS.

7.6 NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY APPLE OR AN APPLE AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE iOS SOFTWARE OR SERVICES PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

8. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL APPLE, ITS AFFILIATES, AGENTS OR PRINCIPALS BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, CORRUPTION OR LOSS OF DATA, FAILURE TO TRANSMIT OR RECEIVE ANY DATA (INCLUDING WITHOUT LIMITATION COURSE INSTRUCTIONS, ASSIGNMENTS AND MATERIALS), BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE iOS SOFTWARE AND SERVICES OR ANY THIRD PARTY SOFTWARE OR APPLICATIONS IN CONJUNCTION WITH THE iOS SOFTWARE OR SERVICES, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Apple’s total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of two hundred and fifty dollars (U.S.$250.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

9. Digital Certificates. The iOS Software contains functionality that allows it to accept digital certificates either issued from Apple or from third parties. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON A CERTIFICATE WHETHER ISSUED BY APPLE OR A THIRD PARTY. YOUR USE OF DIGITAL CERTIFICATES IS AT YOUR SOLE RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, APPLE MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ACCURACY, SECURITY, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH RESPECT TO DIGITAL CERTIFICATES.

10. Export Control. You may not use or otherwise export or re-export the iOS Software except as authorized by United States law and the laws of the jurisdiction(s) in which the iOS Software was obtained. In particular, but without limitation, the iOS Software may not be exported or re-exported (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List or any other restricted party lists. By using the iOS Software, you represent and warrant that you are not located in any such country or on any such list. You also agree that you will not use the iOS Software for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of missiles, nuclear, chemical or biological weapons.

11. Government End Users. The iOS Software and related documentation are "Commercial Items", as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

12. Controlling Law and Severability. This License will be governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles. This License shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If you are a consumer based in the United Kingdom, this License will be governed by the laws of the jurisdiction of your residence. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.

13. Complete Agreement; Governing Language. This License constitutes the entire agreement between you and Apple relating to the iOS Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by Apple. Any translation of this License is done for local requirements and in the event of a dispute between the English and any non-English versions, the English version of this License shall govern, to the extent not prohibited by local law in your jurisdiction.

14. Third Party Acknowledgements. Portions of the iOS Software may utilize or include third party software and other copyrighted material. Acknowledgements, licensing terms and disclaimers for such material are contained in the electronic documentation for the iOS Software, and your use of such material is governed by their respective terms. Use of the Google Safe Browsing Service is subject to the Google Terms of Service (http://www.google.com/terms_of_service.html) and to Google's Privacy Policy (http://www.google.com/privacypolicy.html).

15. Use of MPEG-4; H.264/AVC Notice.
(a) The iOS Software is licensed under the MPEG-4 Systems Patent Portfolio License for encoding

in compliance with the MPEG-4 Systems Standard, except that an additional license and payment of royalties are necessary for encoding in connection with (i) data stored or replicated in physical media which is paid for on a title by title basis and/or (ii) data which is paid for on a title by title basis and is transmitted to an end user for permanent storage and/or use. Such additional license may be obtained from MPEG LA, LLC. See http://www.mpegla.com for additional details.

(b) The iOS Software contains MPEG-4 video encoding and/or decoding functionality. The iOS Software is licensed under the MPEG-4 Visual Patent Portfolio License for the personal and non-commercial use of a consumer for (i) encoding video in compliance with the MPEG-4 Visual Standard ("MPEG-4 Video") and/or (ii) decoding MPEG-4 video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed by MPEG LA to provide MPEG-4 video. No license is granted or shall be implied for any other use. Additional information including that relating to promotional, internal and commercial uses and licensing may be obtained from MPEG LA, LLC. See http://www.mpegla.com.

(c) The iOS Software contains AVC encoding and/or decoding functionality, commercial use of H.264/AVC requires additional licensing and the following provision applies: THE AVC FUNCTIONALITY IN THE iOS SOFTWARE IS LICENSED HEREIN ONLY FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR AVC VIDEO THAT WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. INFORMATION REGARDING OTHER USES AND LICENSES MAY BE OBTAINED FROM MPEG LA L.L.C. SEE HTTP://WWW.MPEGLA.COM.

16. Yahoo Search Service Restrictions. The Yahoo Search Service available through Safari is licensed for use only in the following countries and regions: Argentina, Aruba, Australia, Austria, Barbados, Belgium, Bermuda, Brazil, Bulgaria, Canada, Cayman Islands, Chile, China, Colombia, Cyprus, Czech Republic, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, France, Germany, Greece, Grenada, Guatemala, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Jamaica, Japan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, New Zealand, Nicaragua, Norway, Panama, Peru, Philippines, Poland, Portugal, Puerto Rico, Romania, Singapore, Slovakia, Slovenia, South Korea, Spain, St. Lucia, St. Vincent, Sweden, Switzerland, Taiwan, Thailand, The Bahamas, Trinidad and Tobago, Turkey, UK, Uruguay, US and Venezuela.

17. Microsoft Exchange Notice. The Microsoft Exchange mail setting in the iOS Software is licensed only for over-the-air synchronization of information, such as email, contacts, calendar and tasks, between your iOS and Microsoft Exchange Server or other server software licensed by Microsoft to implement the Microsoft Exchange ActiveSync protocol.

EA1304
07/21/2015

Apple Pay Supplemental Terms and Conditions

These Apple Pay Supplemental Terms and Conditions (the "Supplemental Terms") supplement the iOS Software License Agreement (the "License"); both the terms of the License and these Supplemental Terms govern your use of the Apple Pay feature. Capitalized terms used in these Supplemental Terms have the meanings set forth in the License.

1 Overview and Use Restrictions

Apple Pay allows you to store virtual representations of credit and debit cards, including store credit and debit cards, which are supported by the Apple Pay feature ("Supported Payment Cards") and use supported iOS Devices to make contactless payments in select stores or within apps. Apple Pay also allows you to use rewards cards that are stored in Wallet, including those that contain stored value ("Apple Pay-Enabled Rewards Cards", and together with Supported Payment Cards, "Supported Cards"), to make contactless rewards cards transactions in select stores as part of a contactless payment using Apple Pay. The Apple Pay features of the iOS Software may only be available in select regions, with select card issuers, and with select merchants. Features may vary by region, issuer, and merchant.

In order to use Apple Pay, you must have a card supported by the Apple Pay feature. Supported Cards may change from time to time. Supported Payment Cards require an active iCloud account in order to use this feature. Supported Cards are only available to individuals aged 13 years or older, and may be subject to additional age-based restrictions imposed by iCloud or the Supported Card which you are trying to provision.

Apple Pay is intended for your personal use and you may only provision your own Supported Cards. If you are provisioning a supported corporate card, you represent that you are doing so with the authorization of your employer and you are authorized to bind your employer to these terms of use and all transactions effected by use of this feature.

You agree not to use Apple Pay for illegal or fraudulent purposes, or any other purposes which are prohibited by the License and these Supplemental Terms. You further agree to use Apple Pay in accordance with applicable law and regulation. You agree not to interfere with or disrupt the Apple Pay service (including accessing the service through any automated means), or any servers or networks connected to the service, or any policies, requirements or regulations of networks connected to the service (including any unauthorized access to, use or monitoring of data or traffic thereon).

2 Apple's Relationship With You

Apple Pay enables you to create a virtual representation of your Supported Payment Cards on your supported iOS Device and use Apple Pay-Enabled Rewards Cards as part of a payment, however Apple does not process payments or rewards cards transactions (such as reward accrual and redemption), or have any other control over payments, returns, refunds, rewards, value, discounts or other commerce activity that may arise out of your use of this feature. The terms of cardholder agreements you may have in place with your issuing bank will continue to govern your use of your Supported Payment Cards and their use in connection with Apple Pay. Similarly, your participation in any merchant rewards or stored value programs and your use of Apple Pay-Enabled Rewards Cards in connection with Apple Pay will be subject to such merchant's terms and conditions. Nothing in the License or these Supplemental Terms modifies the terms of any cardholder or merchant agreement, and such terms will govern your use of the applicable Supported Card and its virtual representation on your iOS Device.

You agree that Apple is not a party to your cardholder or merchant agreements, nor is Apple responsible for the content, accuracy or unavailability of any payment cards, rewards cards, stored value cards, commerce activities, transactions or purchases while using Apple Pay functionality, nor is Apple in any way involved in the issuance of credit or assessing eligibility for credit, or the accrual or redemption of rewards under a merchant's rewards program. For all disputes or questions about payment cards, rewards cards, stored value cards, or associated commerce activity, please contact your issuer or the applicable merchant.

3 Privacy

Apple Pay requires some information from your iOS Device in order to offer the full experience.

You can find more information on the data collected, used or shared as part of your use of Apple Pay by reading About Apple Pay and Privacy or by visiting http://www.apple.com/privacy.

4 Security; Lost or Disabled Devices

Apple Pay stores virtual representations of your Supported Payment Cards and should be protected as you would protect your physical credit and debit cards. Providing your device passcode to a third party or allowing a third party to add their fingerprint to use Touch ID may result in their ability to make payments and receive or redeem rewards using Apple Pay on your device.   You are solely responsible for maintaining the security of your device and of your passcode. You agree that Apple does not have any responsibility if you lose or share access to your device. You agree that Apple does not have any responsibility if you make unauthorized modifications to iOS (such as by way of a "jailbreak").

If your device is lost or stolen and you have Find My iPhone enabled, you can use Find My iPhone to attempt to suspend the ability to pay with the virtual credit and debit cards on the device by putting it into Lost Mode. You can also erase your device, which will attempt to suspend the ability to pay with the virtual credit and debit cards on the device and will also attempt to remove the Apple Pay-Enabled Rewards Cards. You should also contact the bank who issued your credit and debit cards and the merchant who issued your rewards or stored value cards in order to prevent unauthorized access to your virtual Supported Cards.

If you report or Apple suspects fraudulent or abusive activity, you agree to cooperate with Apple in any investigation and to use any fraud prevention measures we prescribe.

5 Limitation of Liability

IN ADDITION TO THE DISCLAIMERS OF WARRANTIES AND LIMITATION OF LIABILITY SET FORTH IN THE LICENSE, APPLE DOES NOT ASSUME ANY LIABILITY FOR PURCHASES, PAYMENTS, TRANSACTIONS, OR OTHER COMMERCE ACTIVITY MADE USING THE APPLE PAY FEATURE, AND YOU AGREE TO LOOK SOLELY TO AGREEMENTS YOU MAY HAVE WITH YOUR ISSUING BANK, PAYMENT NETWORK, OR MERCHANT TO RESOLVE ANY QUESTIONS OR DISPUTES RELATING TO YOUR SUPPORTED CARDS, VIRTUAL SUPPORTED CARDS AND ASSOCIATED COMMERCE ACTIVITY.

NOTICES FROM APPLE

If Apple needs to contact you about your product or account, you consent to receive the notices by email. You agree that any such notices that we send you electronically will satisfy any legal communication requirements.

Exhibit 4

TERMS AND CONDITIONS

A. TERMS OF SALE
B. ITUNES STORE TERMS AND CONDITIONS
C. MAC APP STORE, APP STORE, APP STORE FOR APPLE TV AND IBOOKS STORE TERMS AND CONDITIONS
D. APPLE MUSIC TERMS AND CONDITIONS

THE LEGAL AGREEMENTS SET OUT BELOW GOVERN YOUR USE OF THE ITUNES STORE, MAC APP STORE, APP STORE, APP STORE FOR APPLE TV, IBOOKS STORE AND APPLE MUSIC SERVICES ("SERVICES"). TO AGREE TO THESE TERMS, CLICK "AGREE." IF YOU DO NOT AGREE TO THESE TERMS, DO NOT CLICK "AGREE," AND DO NOT USE THE SERVICES.

A. TERMS OF SALE

PAYMENTS, TAXES, AND REFUND POLICY

You agree that you will pay for all products you purchase through the Services, and that Apple may charge your payment method for any products purchased and for any additional amounts (including any taxes and late fees, as applicable) that may be accrued by or in connection with your Account. YOU ARE RESPONSIBLE FOR THE TIMELY PAYMENT OF ALL FEES AND FOR PROVIDING APPLE WITH A VALID PAYMENT METHOD FOR PAYMENT OF ALL FEES. For details of how purchases are billed please visit http://support.apple.com/kb/HT5582.

Your total price will include the price of the product plus any applicable tax; such tax is based on the bill-to address and the tax rate in effect at the time you download the product.

All sales and rentals of products are final.

Prices for products offered via the Services may change at any time, and the Services do not provide price protection or refunds in the event of a price reduction or promotional offering.

If a product becomes unavailable following a transaction but prior to download, your sole remedy is a refund. If technical problems prevent or unreasonably delay delivery of your product, your exclusive and sole remedy is either replacement or refund of the price paid, as determined by Apple.

1-Click®

1-Click is a registered service mark of Amazon.com, Inc., used under license. 1-Click is a convenient feature that allows you to make a purchase from the Services with a single click of your mouse or other input device. When accessing the Services on your computer, 1-Click purchasing may be activated via the dialog that appears when you click a Buy button. (You may reset this selection at any time by clicking Reset Warnings in your Account information). When accessing the Services on your Apple-branded products running iOS such as an iPad, iPod touch, or iPhone (“iOS Device”), 1-Click is activated for each transaction by tapping the button showing the price of the product, which reveals the Buy button. When 1-Click is activated, clicking or tapping the Buy button starts the download immediately and completes your transaction without any further steps.

GIFT CERTIFICATES, ITUNES CARDS AND CODES, ALLOWANCES, AND CONTENT CODES

Gift Certificates, iTunes Cards and Codes, and Allowances are issued and managed by Apple Value Services, LLC (“Issuer”).

Gift Certificates, iTunes Cards and Codes, Content Codes, and Allowances, in addition to unused balances, are not redeemable for cash and cannot be returned for a cash refund (except as required by law); exchanged; resold; used to purchase Gifts, Gift Certificates, or iTunes Cards or Codes; used to provide Allowances; used for purchases on the Apple Online Store; or used in Apple Retail Stores. Unused balances are not transferable.

Gift Certificates, iTunes Cards and Codes, Content Codes, and Allowances purchased in the United States may be redeemed through the Services only in the United States, its territories, and possessions.

The Gift Certificate/iTunes Card/Code cash value is 1/10 of one cent.

Neither Issuer nor Apple is responsible for lost or stolen Gift Certificates, iTunes Cards or Codes, Content Codes, or Allowances. Risk of loss and title for Gift Certificates, iTunes Cards and Codes, and Allowances transmitted electronically pass to the purchaser in Virginia upon electronic transmission to the recipient. Risk of loss and title for Content Codes transmitted electronically pass in California upon electronic transmission from Apple; for avoidance of doubt, such recipient may not always be you.

Apple reserves the right to close accounts and request alternative forms of payment if a Gift Certificate, iTunes Card or Code, Content Code, or Allowance is fraudulently obtained or used on the Service.

APPLE, ISSUER, AND THEIR LICENSEES, AFFILIATES, AND LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO GIFT CERTIFICATES, ITUNES CARDS OR CODES, CONTENT CODES, ALLOWANCES, OR THE ITUNES STORE, APP STORE, MAC APP STORE, OR IBOOKS STORE, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN THE EVENT THAT A GIFT CERTIFICATE, ITUNES CARD OR CODE, CONTENT CODE, OR ALLOWANCE IS NONFUNCTIONAL, YOUR SOLE REMEDY, AND OUR SOLE LIABILITY, SHALL BE THE REPLACEMENT OF SUCH GIFT CERTIFICATE, ITUNES CARD OR CODE, CONTENT CODE, OR ALLOWANCE. THESE LIMITATIONS MAY NOT APPLY TO YOU. CERTAIN STATE LAWS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS, OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY ALSO HAVE ADDITIONAL RIGHTS.

GIFTS

Gifts purchased from the Services may be purchased only for, and redeemed only by, persons in the United States, its territories, and possessions. Gift recipients must have compatible hardware and parental control settings to utilize some gifts.

PRE-ORDERS

By pre-ordering products, you are authorizing the Services to automatically charge your account and download the product when it becomes available. You may cancel your pre-order prior to the time the item becomes available.

FAMILY SHARING

Family Sharing allows you to share eligible iTunes, App Store, Mac App Store, and iBooks Store products with up to six members (including yourself) of a “Family.” If you set up or join a Family, you may view the eligible products of other Family members and download such products to your compatible device or computer. You can also choose to hide purchases so that other Family members will not be able to view or download them from you. You can share information such as photos and videos via the Photos app, events via your Family Calendar, reminders via the Reminders app, location information via Find My Friends, and device location via Find My iPhone. Family Sharing is for personal, non-commercial use only. iTunes and iCloud accounts are required; iOS 8 and/or OS X Yosemite are required to start and join a Family. Certain transactions and features may not be compatible with earlier software and may require a software upgrade. If you join a Family, the features of Family Sharing are enabled on your compatible devices and computers automatically.

The “Organizer” of a Family can invite other members to participate in the Family. The Organizer must be 18 years or older and must have an eligible payment method registered with iTunes. If you are an Organizer, you represent that you are the parent or legal guardian of any Family member under age 13. The Organizer's payment method is used to pay for any purchase initiated by a Family member in excess of any store credit in such initiating Family member’s account. Products are associated with the account of the Family member who initiated the transaction. BY INVITING FAMILY MEMBERS TO JOIN A FAMILY, THE ORGANIZER AGREES THAT ALL FAMILY MEMBER PURCHASES ARE AUTHORIZED BY AND ARE THE RESPONSIBILITY OF THE ORGANIZER, EVEN IF THE ORGANIZER WAS UNAWARE OF ANY PARTICULAR PURCHASE, IF A FAMILY MEMBER EXCEEDED HIS OR HER AUTHORITY AS GRANTED BY THE ORGANIZER, OR IF MULTIPLE FAMILY MEMBERS PURCHASE THE SAME PRODUCT. THE ORGANIZER IS RESPONSIBLE FOR COMPLIANCE WITH ANY AGREEMENT WITH ITS PAYMENT METHOD PROVIDER, AND ASSUMES ALL RISK IN THE EVENT THAT SHARING ACCESS TO SUCH PAYMENT METHOD LIMITS ANY PROTECTION OFFERED BY THE PAYMENT METHOD PROVIDER. The Organizer can change the payment method on file at any time. A record of the purchase will be sent to the initiating Family member and the Organizer, even if the purchase is hidden by the Family member; please use Report a Problem on your receipt if you or your Family members do not recognize charges on your receipt or payment method statement.

The Organizer can use the Ask to Buy function to require children under the age of 18 to obtain permission from the Organizer, and/or other adults designated by the Organizer, to download free or paid products before a purchase or download commences. Products downloaded from Family members and products acquired via redemption codes are not subject to Ask to Buy. If you are an Organizer, you represent that you and/or any adult designee is the parent or legal guardian of any Family member for whom Ask to Buy is activated. Ask to Buy is optimized for iOS 8 and OS X Yosemite; product purchase or download requests from earlier software may present users with an alternative permission process or prevent purchases altogether, and may require a software upgrade. Apple is not responsible for any harm resulting from a delay in Ask to Buy approvals or denials.

The Organizer may remove any Family member from the Family, which will terminate that Family member's ability to initiate authorized purchases on the Organizer's payment method, and that Family Member’s ability to view and share other Family members' products and information. When a Family member leaves or is removed from a Family, the remaining Family members may no longer be able to view or download the departing member’s products or information, or access products previously downloaded from the departing Family member, including purchases made on the Organizer's payment method while the departing member was part of the Family. Similarly, if you leave a Family, you may no longer be able to view or download the products or information of the other Family members, and products that you downloaded from other Family members while a member of the Family may no longer be accessible. If you have made In-App Purchases from an app originally purchased by a departed Family member or downloaded from a Family member and you no longer belong to the Family, you need to purchase the app yourself and restore the In-App Purchases to regain access to them; please review the developer’s policies and the section of this Agreement entitled “In-App Purchases” before buying In-App Purchases. Because personal accounts for users under age 13 can only be created as part of Family Sharing, deleting such an account in order to remove it from the Family will terminate that Family member’s Apple ID and his or her ability to access any Apple services that require an Apple ID or any content associated with that Apple ID.

You can only belong to one Family at a time, and may join any Family no more than twice per year. You can change the store account you associate with a Family no more than once every 90 days. All Family members must use the same iTunes Store country or region. Music, movies, TV shows and books can be downloaded from the iTunes Service on up to 10 devices per account, only five of which can be computers; eligible apps can be downloaded to any devices the Family member owns or controls. Not all products, including In-App Purchases, content that is not available for re-download, subscriptions, and some previously purchased apps, are eligible for Family Sharing. Apple reserves the right to disband a Family in accordance with the “Termination” section of this Agreement.

ELECTRONIC CONTRACTING

Your use of the Services includes the ability to enter into agreements and/or to make transactions electronically. YOU ACKNOWLEDGE THAT YOUR ELECTRONIC SUBMISSIONS CONSTITUTE YOUR AGREEMENT AND INTENT TO BE BOUND BY AND TO PAY FOR SUCH AGREEMENTS AND TRANSACTIONS. YOUR AGREEMENT AND INTENT TO BE BOUND BY ELECTRONIC SUBMISSIONS APPLIES TO ALL RECORDS RELATING TO ALL TRANSACTIONS YOU ENTER INTO ON THIS SITE, INCLUDING NOTICES OF CANCELLATION, POLICIES, CONTRACTS, AND APPLICATIONS. In order to access and retain your electronic records, you may be required to have certain hardware and software, which are your sole responsibility.

NON-APPLE DEVICES

If you sign up for an Account or use a Service covered by this Agreement on a non-Apple-branded device or computer, you may have access to only a limited set of Account or Service functionality. As a condition to accessing your Account or a Service on a non-Apple-branded device or computer, you agree to all relevant terms and conditions found in this Agreement, including, without limitation, all requirements for use of an Account or Service, limitations on use, availability, disclaimers of warranties, rules regarding your content and conduct, and termination. Terms found in this Agreement relating to features or Services not available for non-Apple-branded device or computer users will not be applicable to you. These include, for example, the App Store. If you later choose to access your Account or a Service from an Apple-branded device or Apple-branded computer, you agree that all of the terms and conditions contained herein apply to your use of such Account or Service.

Apple is not responsible for typographic errors.

B. ITUNES STORE TERMS AND CONDITIONS

THIS LEGAL AGREEMENT BETWEEN YOU AND APPLE INC. ("APPLE") GOVERNS YOUR USE OF THE ITUNES STORE SERVICE (THE “ITUNES SERVICE”).

THE ITUNES STORE SERVICE

Apple is the provider of the iTunes Service, which permits you to access, purchase or rent digital content ("iTunes Products") for end user use only under the terms and conditions set forth in this Agreement.

REQUIREMENTS FOR USE OF THE ITUNES SERVICE

Only persons age 13 years or older can create accounts. Accounts for persons under 13 years old can be created by a parent or legal guardian using Family Sharing or by an approved educational institution. Children under the age of majority should review this Agreement with their parent or guardian to ensure that the child and parent or legal guardian understand it.

The iTunes Service is available to you only in the United States, its territories, and possessions. You agree not to use or attempt to use the iTunes Service from outside these locations. Apple may use technologies to verify your compliance.

Use of the iTunes Service requires compatible devices, Internet access, and certain software (fees may apply); may require periodic updates; and may be affected by the performance of these factors. High-speed Internet access is strongly recommended for regular use and is required for video. The latest version of required software is recommended to access the iTunes Service and may be required for certain transactions or features and to download iTunes Products previously purchased or acquired from the iTunes Service. You agree that meeting these requirements, which may change from time to time, is your responsibility. The iTunes Service is not part of any other product or offering, and no purchase or obtaining of any other product shall be construed to represent or guarantee you access to the iTunes Service.

YOUR ACCOUNT

As a registered user of the iTunes Service, you may establish an account ("Account"). Don’t reveal your Account information to anyone else. You are solely responsible for maintaining the confidentiality and security of your Account and for all activities that occur on or through your Account, and you agree to immediately notify Apple of any security breach of your Account. Apple shall not be responsible for any losses arising out of the unauthorized use of your Account.

In order to purchase and download iTunes Products from the iTunes Service, you must enter your Apple ID and password or use Touch ID to authenticate your Account for transactions. Once you have authenticated your Account using your Apple ID and password, you will not need to authenticate again for fifteen minutes on your computer or iOS Device; you can choose to allow your computer or Apple TV to remember your password to remain authenticated. During this time, you will be able to purchase and download iTunes Products without re-entering your password. You can turn off the ability to make iTunes Product transactions or change settings to require a password for every transaction by adjusting the settings on your computer, iOS Device, or Apple TV. For more information, please see http://support.apple.com/kb/HT1904 and http://support.apple.com/kb/HT4213.

You agree to provide accurate and complete information when you register with, and as you use, the iTunes Service ("iTunes Registration Data"), and you agree to update your iTunes Registration Data to keep it accurate and complete. You agree that Apple may store and use the iTunes Registration Data you provide for use in maintaining and billing fees to your Account.

AUTOMATIC DELIVERY AND DOWNLOADING PREVIOUS PURCHASES

When you first acquire music, purchased (i.e. not rented) movie, TV show and music video iTunes Products (collectively, “iTunes Eligible Content”), you may elect to automatically receive (“auto-download”) copies of such iTunes Eligible Content on additional compatible iOS Devices (except for purchased movies and TV show iTunes Products) and iTunes-authorized computers with compatible software by associating such iOS Devices and computers subject to the association rules below (each, an “Associated Device”). For each Associated Device, you may specify which type of iTunes Eligible Content, if any, may be auto-downloaded to it. On an Associated Device that is capable of receiving push notifications (“Push-Enabled”), including iOS Devices, the iTunes Eligible Content will auto-download to that Associated Device when it has an Internet connection; on an Associated Device that is not Push-Enabled, iTunes Eligible Content will automatically appear in the download queue and you may manually initiate the download within iTunes.

As an accommodation to you, subsequent to acquiring iTunes Eligible Content, you may download certain of such previously-acquired iTunes Eligible Content onto any Associated Device. Some iTunes Eligible Content that you previously acquired may not be available for subsequent download at any given time, and Apple shall have no liability to you in such event. As you may not be able to subsequently download certain previously-acquired iTunes Eligible Content, once you download an item of iTunes Eligible Content, it is your responsibility not to lose, destroy, or damage it, and you may want to back it up.

Association of Associated Devices is subject to the following terms:

(i) You may auto-download iTunes Eligible Content or download previously-acquired iTunes Eligible Content from an Account on up to 10 Associated Devices, provided no more than 5 are iTunes-authorized computers.

(ii) An Associated Device can be associated with only one Account at any given time.

(iii) You may switch an Associated Device to a different Account only once every 90 days.

(iv) You may download previously-acquired free content onto an unlimited number of devices while it is free on the iTunes Service, but on no more than 5 iTunes-authorized computers.

An Apple TV is not an "Associated Device." However, TV show iTunes Products and purchased (i.e. not rented) movies iTunes Products may be played back on compatible Apple TVs, provided that you may only play back any such TV show or movie on a limited number of Apple TVs at the same time.

Some pieces of iTunes Eligible Content may be large, and significant data charges may result from delivery of such iTunes Eligible Content over a data connection.

ITUNES MATCH

iTunes Match permits you to remotely access your matched or uploaded songs, and music videos you have purchased with your Account, along with related metadata, playlists, and other information about your iTunes Library ("iTunes Match Content").

You may subscribe to iTunes Match for an annual fee. You must have a valid credit card on file with iTunes to subscribe. The subscription is non-refundable (except as required by applicable law), and will automatically renew for one-year periods until you cancel. Your account will be charged no more than 24 hours prior to the expiration of the current subscription period. You may cancel automatic renewal by adjusting the iTunes Store account settings on your computer. You will no longer be able to access your iTunes Match Content from iTunes Match after the end of your subscription period.

iTunes Match works with libraries that contain up to 100,000 songs which are either (i) not currently available on the iTunes Service, or (ii) not purchased from the iTunes Service with your Account. Songs that do not meet certain quality criteria or that are not authorized for your computer are not eligible for iTunes Match.

In order to set up and use iTunes Match, information about the media in your iTunes library, your operating system and hardware identifiers, will be collected and associated with your Account on Apple's servers. iTunes Match automatically scans the song files and collects other information that may be used to identify media in your iTunes library, such as the names of songs, song artists or song durations. iTunes Match will use this information to match songs to those currently available on the iTunes Store, and will make matched songs available to you in a format then available on the iTunes Store. If the song is not successfully matched, your copy of the song will be uploaded to Apple in the same format or a format determined by Apple. Apple reserves the right to limit types of content uploaded (for example, excessively large files). Matched or uploaded songs and related metadata will be available for access from an Associated Device that has been enabled for iTunes Match. Association of Associated Devices for iTunes Match is subject to the same terms as Automatic Delivery and Downloading Previous Purchases, and uploaded or matched songs and related information are deemed to be "iTunes Eligible Content." You may also access iTunes Match Content from compatible Apple TVs, provided that you may only do so on a limited number of Apple TVs at the same time.

When you use iTunes Match, Apple will log information such as the tracks you play, stop or skip, the devices you use, and the time and duration of playback. By using iTunes Match, you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this information, including your iTunes Match usage information, to report to licensors and pay royalties, provide and improve iTunes features and services and other Apple products and services, and as otherwise permitted in accordance with Apple's Privacy Policy, available here: http://www.apple.com/legal/privacy/.

You hereby agree to use iTunes Match only for lawfully acquired content. Any use for illegitimate content infringes the rights of others and may subject you to civil and criminal penalties, including possible monetary damages, for copyright infringement.

iTunes Match is provided on an "AS IS" basis and may contain errors or inaccuracies that could cause failures, corruption or loss of data and/or information, including music, playlist, and play history, from your computer or device and from peripherals (including, without limitation, servers and other computers) connected thereto. You should back up all data and information on your computer or device and any peripherals prior to using iTunes Match. You expressly acknowledge and agree that all use of iTunes Match is at your sole risk. To the extent permitted by law, Apple shall have no liability with respect to your use of iTunes Match, including the inability to access matched or uploaded content.

PRIVACY

The iTunes Service is subject to Apple's Privacy Policy at http://www.apple.com/legal/privacy/.

When you opt in to the Genius feature, Apple will, from time to time, automatically collect information that can be used to identify media in your iTunes library on any Genius-enabled device, such as your play history and playlists. This includes media purchased or acquired through iTunes and media obtained from other sources. This information will be stored anonymously and will not be associated with your name or Account. When you use the Genius feature, Apple will use this information and the contents of your iTunes library, as well as other information, to give personalized recommendations to you.

Apple may only use this information and combine it with aggregated information from the iTunes libraries of other users who also opt in to this feature, your iTunes Store purchase history data, aggregated purchase history data from other iTunes Store users, and other information obtained from third parties, to:

• Create personalized playlists for you from your iTunes library.

• Provide you with recommendations regarding media and other products and services that you may wish to purchase or acquire.

• Provide recommendations regarding products and services to other users.

At all times your information will be treated in accordance with Apple's Privacy Policy.

Once you opt in to the Genius feature, you will be able to create Genius playlists on Genius-capable devices.

If you prefer that we do not collect and use information from your iTunes library in this manner, you should not enable the Genius feature. You can revoke your opt-in choice at any time by turning off the Genius feature from the Store menu in iTunes on your computer or turning off Genius in the Settings on your device. After you opt out, iTunes will no longer send information about your iTunes library to Apple. If you have elected to share your library from multiple devices, you need to turn off the Genius feature from each device.

By opting in to the Genius feature, you consent to the use of your information as described above and as described in Apple's Privacy Policy.

CONTENT AVAILABILITY

Apple reserves the right to change content options (including eligibility for particular features) without notice. For further information or concerns about closed captioning in specific content within the iTunes Store, please email accessibility@apple.com. You may also contact Thomas Montgomery, Accessibility Response Engineer, 1 Infinite Loop, Cupertino, California 95014, Phone/Fax: 408-783-5512.

USE OF CONTENT

You agree that the iTunes Service and certain iTunes Products include security technology that limits your use of iTunes Products and that, whether or not iTunes Products are limited by security technology, you shall use iTunes Products in compliance with the applicable usage rules established by Apple and its licensors ("Usage Rules"), and that any other use of the iTunes Products may constitute a copyright infringement. Any security technology is an inseparable part of the iTunes Products. Apple reserves the right to modify the Usage Rules at any time. You agree not to violate, circumvent, reverse-engineer, decompile, disassemble, or otherwise tamper with any of the security technology related to such Usage Rules for any reason—or to attempt or assist another person to do so. Usage Rules may be controlled and monitored by Apple for compliance purposes, and Apple reserves the right to enforce the Usage Rules without notice to you. You agree not to access the iTunes Service by any means other than through software that is provided by Apple for accessing the iTunes Service. You shall not access or attempt to access an Account that you are not authorized to access. You agree not to modify the software in any manner or form, or to use modified versions of the software, for any purposes including obtaining unauthorized access to the iTunes Service. Violations of system or network security may result in civil or criminal liability.

USAGE RULES

(i) You shall be authorized to use iTunes Products only for personal, noncommercial use.

(ii) You shall be authorized to use iTunes Products on five iTunes-authorized devices at any time, except for Content Rentals (see below).

(iii) You shall be able to store iTunes Products from up to five different Accounts at a time on compatible devices, provided that each iPhone may sync tone iTunes Products with only a single iTunes-authorized device at a time, and syncing an iPhone with a different iTunes-authorized device will cause tone iTunes Products stored on that iPhone to be erased.

(iv) You shall be authorized to burn an audio playlist up to seven times.

(v) You shall not be entitled to burn video iTunes Products or tone iTunes Products.

(vi) iTunes Plus Products do not contain security technology that limits your usage of such products, and Usage Rules (ii) - (v) do not apply to iTunes Plus Products. You may copy, store, and burn iTunes Plus Products as reasonably necessary for personal, noncommercial use.

(vii) You shall be able to manually sync a movie from at least one iTunes-authorized device to devices that have manual sync mode, provided that the movie is associated with an Account on the primary iTunes-authorized device, where the primary iTunes-authorized device is the one that was first synced with the device or the one that you subsequently designate as primary using iTunes.

(viii) An HDCP connection is required to view content transmitted over HDMI.

(ix) Content Rentals

(a) Content rentals are viewable on only one device at a time. You must be connected to the iTunes Service when moving rentals, and you may do so only between your computer and other compatible devices. Content rented using your Apple TV, iPad, iPhone 4, or iPod touch (4th generation) may not be moved. If you move a rental to a compatible device and then use the iTunes Service to restore that device, or choose Settings > Reset > Erase all content and settings on that device, the rental will be permanently deleted.

(b) Once you purchase a rental, you must fully download the rental within thirty (30) days. You have thirty (30) days after downloading a rental to begin viewing. Once you begin viewing, you have twenty-four (24) hours to finish viewing a movie. Stopping, pausing, or restarting a rental does not extend the available time for viewing.

Some iTunes Products, including but not limited to Content rentals, may be downloaded only once and cannot be replaced if lost for any reason. It is your responsibility not to lose, destroy, or damage iTunes Products once downloaded, and you may wish to back them up.

The delivery of iTunes Products does not transfer to you any commercial or promotional use rights in the iTunes Products. Any burning or exporting capabilities are solely an accommodation to you and shall not constitute a grant, waiver, or other limitation of any rights of the copyright owners in any content embodied in any iTunes Product.

You acknowledge that, because some aspects of the iTunes Service, iTunes Products, and administration of the Usage Rules entails the ongoing involvement of Apple, if Apple changes any part of or discontinues the iTunes Service, which Apple may do at its election, you may not be able to use iTunes Products to the same extent as prior to such change or discontinuation, and that Apple shall have no liability to you in such case.

SEASON PASS, MULTI-PASS, ITUNES PASS

The full price of the Season Pass, Multi-Pass, or iTunes Pass is charged upon purchase. You must connect to the iTunes Service and download any remaining Pass content within 90 days after the final Pass content becomes available (or such other time period as may be specified on the purchase page), after which that content may no longer be available for download as part of the purchase. If automatic renewal is selected when you purchase a Multi-Pass, you will be charged the full price of each subsequent Multi-Pass cycle, unless and until you cancel automatic renewal prior to the beginning of the subsequent Multi-Pass cycle (in the Manage Passes section of your Account information). If a network or studio delivers fewer TV episodes than planned when you purchased a Season Pass, we will credit to your Account the retail value of the corresponding number of episodes.

HIGH-DEFINITION (HD) ITUNES PRODUCTS

HD iTunes Products are viewable only on HD capable devices; however, HD iTunes Products purchased (not rented) include a standard-definition version for use on non-HD devices.

SUBMISSIONS TO THE ITUNES SERVICE

The iTunes Service may offer interactive features that allow you to submit materials (including links to third-party content) on areas of the iTunes Service accessible and viewable by the public. You agree that any use by you of such features, including any materials submitted by you, shall be your sole responsibility, shall not infringe or violate the rights of any other party or violate any laws, contribute to or encourage infringing or otherwise unlawful conduct, or otherwise be obscene, objectionable, or in poor taste. You also agree that you have obtained all necessary rights and licenses. You agree to provide accurate and complete information in connection with your submission of any materials on the iTunes Service. You hereby grant Apple a worldwide, royalty-free, nonexclusive license to use such materials as part of the iTunes Service or in relation to iTunes Products, without any compensation or obligation to you. Apple reserves the right to not post or publish any materials, and to remove or edit any material, at any time in its sole discretion without notice or liability.

Apple has the right, but not the obligation, to monitor any materials submitted by you or otherwise available on the iTunes Service, to investigate any reported or apparent violation of this Agreement, and to take any action that Apple in its sole discretion deems appropriate, including, without limitation, termination hereunder or under Apple's Copyright Policy (http://www.apple.com/legal/copyright.html).

THIRD-PARTY MATERIALS

Certain content, iTunes Products, and services available via the iTunes Service may include materials from third parties. Apple may provide links to third-party websites as a convenience to you. You agree that Apple is not responsible for examining or evaluating the content or accuracy and Apple does not warrant and will not have any liability or responsibility for any third-party materials or websites, or for any other materials, products, or services of third parties. You agree that you will not use any third-party materials in a manner that would infringe or violate the rights of any other party and that Apple is not in any way responsible for any such use by you.

OBJECTIONABLE MATERIAL

You understand that by using the iTunes Service, you may encounter material that you may deem to be offensive, indecent, or objectionable, and that such content may or may not be identified as having explicit material. Nevertheless, you agree to use the iTunes Service at your sole risk and Apple shall have no liability to you for material that may be found to be offensive, indecent, or objectionable. iTunes Product types and descriptions are provided for convenience, and you agree that Apple does not guarantee their accuracy.

IMPORTANT SAFETY INFORMATION

To avoid muscle, joint, or eye strain during your use of the products offered through the iTunes Service, you should always take frequent breaks, and take a longer rest if you experience any soreness, fatigue, or discomfort. A very small percentage of people may experience seizures or blackouts when exposed to flashing lights or patterns, including but not limited to while playing video games or watching videos. Symptoms may include dizziness, nausea, involuntary movements, loss of awareness, altered vision, tingling, numbness, or other discomforts. Consult a doctor before using the products offered through the iTunes Service if you have ever suffered these or similar symptoms, and stop using such products immediately and see a doctor if they occur during your use of such products. Parents should monitor their children's use of the products offered through the iTunes Service for signs of symptoms.

INTELLECTUAL PROPERTY

You agree that the iTunes Service, including but not limited to iTunes Products, graphics, user interface, audio clips, video clips, editorial content, and the scripts and software used to implement the iTunes Service, contains proprietary information and material that is owned by Apple and/or its licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright. You agree that you will not use such proprietary information or materials in any way whatsoever except for use of the iTunes Service in compliance with this Agreement. No portion of the iTunes Service may be reproduced in any form or by any means, except as expressly permitted in these terms. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the iTunes Service in any manner, and you shall not exploit the iTunes Service in any unauthorized way whatsoever, including, but not limited to, by trespass or burdening network capacity.

Notwithstanding any other provision of this Agreement, Apple and its licensors reserve the right to change, suspend, remove, or disable access to any iTunes Products, content, or other materials comprising a part of the iTunes Service at any time without notice. In no event will Apple be liable for making these changes. Apple may also impose limits on the use of or access to certain features or portions of the iTunes Service, in any case and without notice or liability.

All copyrights in and to the iTunes Service (including the compilation of content, postings, links to other Internet resources, and descriptions of those resources) and related software are owned by Apple and/or its licensors, who reserve all their rights in law and equity. THE USE OF THE SOFTWARE OR ANY PART OF THE ITUNES SERVICE, EXCEPT FOR USE OF THE ITUNES SERVICE AS PERMITTED IN THIS AGREEMENT, IS STRICTLY PROHIBITED AND INFRINGES ON THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS AND MAY SUBJECT YOU TO CIVIL AND CRIMINAL PENALTIES, INCLUDING POSSIBLE MONETARY DAMAGES, FOR COPYRIGHT INFRINGEMENT.

Apple, the Apple logo, iTunes, and other Apple trademarks, service marks, graphics, and logos used in connection with the iTunes Service are trademarks or registered trademarks of Apple Inc. in the U.S. and/or other countries. Other trademarks, service marks, graphics, and logos used in connection with the iTunes Service may be the trademarks of their respective owners. You are granted no right or license with respect to any of the aforesaid trademarks and any use of such trademarks.

As an Account holder of the iTunes Service in good standing, you may be provided with limited access to download certain album cover art for music stored in the iTunes Library of your iTunes application. Such access is provided as an accommodation only, and Apple does not warrant, and will not have any liability or responsibility for, such album cover art or your use thereof. You may access album cover art only for music for which you are the lawful owner of a legal copy. Album cover art is provided for personal, noncommercial use only. You agree that you will not use album cover art in any manner that would infringe or violate this Agreement or the rights of any other party, and that Apple is not in any way responsible for any such use by you.

TERMINATION

If you fail, or Apple suspects that you have failed, to comply with any of the provisions of this Agreement, Apple, at its sole discretion, without notice to you may: (i) terminate this Agreement and/or your Account, and you will remain liable for all amounts due under your Account up to and including the date of termination; and/or (ii) terminate the license to the software; and/or (iii) preclude access to the iTunes Service (or any part thereof).

Apple reserves the right to modify, suspend, or discontinue the iTunes Service (or any part or content thereof) at any time with or without notice to you, and Apple will not be liable to you or to any third party should it exercise such rights.

DISCLAIMER OF WARRANTIES; LIABILITY LIMITATION

APPLE DOES NOT GUARANTEE, REPRESENT, OR WARRANT THAT YOUR USE OF THE ITUNES SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE, AND YOU AGREE THAT FROM TIME TO TIME APPLE MAY REMOVE THE ITUNES SERVICE FOR INDEFINITE PERIODS OF TIME, OR CANCEL THE ITUNES SERVICE AT ANY TIME, WITHOUT NOTICE TO YOU.

YOU EXPRESSLY AGREE THAT YOUR USE OF, OR INABILITY TO USE, THE ITUNES SERVICE IS AT YOUR SOLE RISK. THE ITUNES SERVICE AND ALL PRODUCTS AND SERVICES DELIVERED TO YOU THROUGH THE ITUNES SERVICE ARE (EXCEPT AS EXPRESSLY STATED BY APPLE) PROVIDED "AS IS" AND "AS AVAILABLE" FOR YOUR USE, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, THE ABOVE EXCLUSION OF IMPLIED WARRANTIES MAY NOT APPLY TO YOU.

IN NO CASE SHALL APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, OR LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM YOUR USE OF ANY OF THE ITUNES SERVICE OR FOR ANY OTHER CLAIM RELATED IN ANY WAY TO YOUR USE OF THE ITUNES SERVICE, INCLUDING, BUT NOT LIMITED TO, ANY ERRORS OR OMISSIONS IN ANY CONTENT, OR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT (OR PRODUCT) POSTED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE ITUNES SERVICE, EVEN IF ADVISED OF THEIR POSSIBILITY. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR THE LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, APPLE'S LIABILITY SHALL BE LIMITED TO THE EXTENT PERMITTED BY LAW.

APPLE SHALL USE REASONABLE EFFORTS TO PROTECT INFORMATION SUBMITTED BY YOU IN CONNECTION WITH THE ITUNES SERVICE, BUT YOU AGREE THAT YOUR SUBMISSION OF SUCH INFORMATION IS AT YOUR SOLE RISK, AND APPLE HEREBY DISCLAIMS ANY AND ALL LIABILITY TO YOU FOR ANY LOSS OR LIABILITY RELATING TO SUCH INFORMATION IN ANY WAY.

APPLE DOES NOT REPRESENT OR GUARANTEE THAT THE ITUNES SERVICE WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND APPLE DISCLAIMS ANY LIABILITY RELATING THERETO. SOME PRODUCTS CAN BE DOWNLOADED ONLY ONCE; AFTER BEING DOWNLOADED, THEY CANNOT BE REPLACED IF LOST FOR ANY REASON. YOU SHALL BE RESPONSIBLE FOR BACKING UP YOUR OWN SYSTEM, INCLUDING ANY ITUNES PRODUCTS PURCHASED, ACQUIRED OR RENTED FROM THE ITUNES STORE.

WAIVER AND INDEMNITY

BY USING THE ITUNES SERVICE, YOU AGREE, TO THE EXTENT PERMITTED BY LAW, TO INDEMNIFY AND HOLD APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, AND LICENSORS HARMLESS WITH RESPECT TO ANY CLAIMS ARISING OUT OF YOUR BREACH OF THIS AGREEMENT, YOUR USE OF THE ITUNES SERVICE, OR ANY ACTION TAKEN BY APPLE AS PART OF ITS INVESTIGATION OF A SUSPECTED VIOLATION OF THIS AGREEMENT OR AS A RESULT OF ITS FINDING OR DECISION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS MEANS THAT YOU CANNOT SUE OR RECOVER ANY DAMAGES FROM APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, AND LICENSORS AS A RESULT OF ITS DECISION TO REMOVE OR REFUSE TO PROCESS ANY INFORMATION OR CONTENT, TO WARN YOU, TO SUSPEND OR TERMINATE YOUR ACCESS TO THE ITUNES SERVICE, OR TO TAKE ANY OTHER ACTION DURING THE INVESTIGATION OF A

SUSPECTED VIOLATION OR AS A RESULT OF APPLE'S CONCLUSION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS WAIVER AND INDEMNITY PROVISION APPLIES TO ALL VIOLATIONS DESCRIBED IN OR CONTEMPLATED BY THIS AGREEMENT.

CHANGES

Apple reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on your use of the iTunes Service. Such modifications and additional terms and conditions will be effective immediately and incorporated into this Agreement. Your continued use of the iTunes Service will be deemed acceptance thereof.

MISCELLANEOUS

This Agreement constitutes the entire agreement between you and Apple and governs your use of the iTunes Service, superseding any prior agreements between you and Apple. You also may be subject to additional terms and conditions that may apply when you use affiliate services, third-party content, or third-party software. If any part of this Agreement is held invalid or unenforceable, that portion shall be construed in a manner consistent with applicable law to reflect, as nearly as possible, the original intentions of the parties, and the remaining portions shall remain in full force and effect. Apple's failure to enforce any right or provisions in this Agreement will not constitute a waiver of such or any other provision. Apple will not be responsible for failures to fulfill any obligations due to causes beyond its control.

The iTunes Service is operated by Apple from its offices in the United States. You agree to comply with all local, state, federal, and national laws, statutes, ordinances, and regulations that apply to your use of the iTunes Service. All transactions on the iTunes Service are governed by California law, without giving effect to its conflict of law provisions. Your use of the iTunes Service may also be subject to other laws. You expressly agree that exclusive jurisdiction for any claim or dispute with Apple or relating in any way to your use of the iTunes Service resides in the courts in the State of California. Risk of loss and title for all electronically delivered transactions pass to the purchaser in California upon electronic transmission to the recipient. No Apple employee or agent has the authority to vary this Agreement.

Apple may notify you with respect to the iTunes Service by sending an email message to your Account email address or a letter via postal mail to your Account mailing address, or by a posting on the iTunes Service. Notices shall become effective immediately.

Apple reserves the right to take steps Apple believes are reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement. You agree that Apple has the right, without liability to you, to disclose any Registration Data and/or Account information to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement (including but not limited to Apple's right to cooperate with any legal process relating to your use of the iTunes Service and/or iTunes Products, and/or a third-party claim that your use of the iTunes Service and/or iTunes Products is unlawful and/or infringes such third party's rights).

C. MAC APP STORE, APP STORE, APP STORE FOR APPLE TV, AND IBOOKS STORE TERMS AND CONDITIONS

THIS LEGAL AGREEMENT BETWEEN YOU AND APPLE INC. ("APPLE") GOVERNS YOUR USE OF THE MAC APP STORE, APP STORE, APP STORE FOR APPLE TV, AND IBOOKS STORE SERVICES (THE “APP AND BOOK SERVICES”).

THE MAC APP STORE, APP STORE, APP STORE FOR APPLE TV AND IBOOKS STORE SERVICES

Apple is the provider of the App and Book Services that permit you to license software products and digital content (the “App and Book Products”) for end user use only under the terms and conditions set forth in this Agreement. For App Store Products (defined below), end users may be individuals acting in their own capacities, commercial enterprises or educational institutions.

REQUIREMENTS FOR USE OF THE APP AND BOOK SERVICES

Only persons age 13 years or older can create accounts. Accounts for persons under 13 years old can be created by a parent or legal guardian using Family Sharing or by an approved educational institution. Children under the age of majority should review this Agreement with their parent or guardian to ensure that the child and the parent or legal guardian understand it.

The App and Book Services are available to you only in the United States, its territories, and possessions. You agree not to use or attempt to use the App and Book Services from outside these locations. Apple may use technologies to verify your compliance.

Use of the App and Book Services requires compatible devices, Internet access, and certain software (fees may apply); may require periodic updates and/or on-demand download of content based on app usage and resource constraints (which may use cellular data); and may be affected by the performance of these factors. High-speed Internet access is strongly recommended. The latest version of required software (including, but not limited to iOS, iTunes and/or Mac App Store software) is recommended to access the App and Book Services and may be required for certain transactions or features and to download App and Book Products previously purchased or acquired from the App and Book Services. You agree that meeting these requirements, which may change from time to time, is your responsibility. The App and Book Services are not part of any other product or offering, and no purchase or obtaining of any other product shall be construed to represent or guarantee you access to the App and Book Services.

YOUR ACCOUNT

As a registered user of the App and Book Services, you may establish an account ("Account"). Don't reveal your Account information to anyone else. You are solely responsible for maintaining the confidentiality and security of your Account, and for all activities that occur on or through your Account, and you agree to immediately notify Apple of any security breach of your Account. Apple shall not be responsible for any losses arising out of the unauthorized use of your Account.

In order to purchase and download App and Book Products from the App and Book Services, you must enter your Apple ID and password or use Touch ID to authenticate your Account for transactions. Once you have authenticated your Account using your Apple ID and password, you will not need to authenticate again for fifteen minutes; during this time, you will be able to purchase and download App and Book Products without re-entering your password. You may also choose to require entry of your password for each transaction and, separately to have your device remember your password for free transactions only. You can turn off the ability to make App and Book Product transactions or change settings to require a password for every App and Book Product transaction by adjusting the settings on your device. For more information, please see http://support.apple.com/kb/HT1904 and http://support.apple.com/kb/HT4213.

You agree to provide accurate and complete information when you register with, and as you use, the App and Book Services ("App and Book Registration Data"), and you agree to update your App and Book Registration Data to keep it accurate and complete. You agree that Apple may store and use the App and Book Registration Data you provide for use in maintaining and billing fees to your Account.

AUTOMATIC DELIVERY AND DOWNLOADING PREVIOUS PURCHASES

When you first acquire App and Book Products (excluding products acquired from the Mac App Store) through the App and Book Services (collectively, "Eligible Content"), you may elect to automatically receive ("auto-download") copies of such Eligible Content on additional compatible Apple-branded hardware with compatible software by associating such hardware subject to the association rules below (each, an "Associated Device"). For each Associated Device, you may specify which type of Eligible Content, if any, may be auto-downloaded to it. On an Associated Device that is capable of receiving push notifications ("Push-Enabled"), including iOS Devices, the Eligible Content will auto-download to that Associated Device when it has an Internet connection; on an Associated Device that is not Push-Enabled, including those running on the Windows operating system, Eligible Content will automatically appear in the download queue and you may manually initiate the download within iTunes.

As an accommodation to you, subsequent to acquiring Eligible Content, you may download certain of such previously-acquired Eligible Content onto any Associated Device. Some Eligible Content that you previously acquired may not be available for subsequent download at any given time, and Apple shall have no liability to you in such event. As you may not be able to subsequently download certain previously-acquired Eligible Content, once you download an item of Eligible Content, it is your responsibility not to lose, destroy, or damage it, and you may want to back it up.

Association of Associated Devices is subject to the following terms:

(i) You may auto-download Eligible Content or download previously-acquired Eligible Content from an Account on up to 10 Associated Devices, provided no more than 5 are iTunes-authorized computers.

(ii) An Associated Device can be associated with only one Account at any given time.

(iii) You may switch an Associated Device to a different Account only once every 90 days.

(iv) You may download previously-acquired free content onto an unlimited number of devices while it is free on the App and Book Services, but on no more than 5 iTunes-authorized computers.

The above terms (i) to (iv) do not apply to App Store Products.

Some pieces of Eligible Content may be large or may initiate the ongoing delivery of content based on usage and resource constraints, and significant data charges may result from delivery of such Eligible Content over a data connection.

AUTOMATIC DELIVERY OF UPDATES

Your device or computer will periodically check with the App Store, App Store for Apple TV and Mac App Store for updates to the apps on your device or computer and, if available, the update may automatically download and install. Certain App Store Products may also download additional content, such as game levels or chapters, on an on-going basis based on usage and resource constraints. You agree that Apple, through the App Store, App Store for Apple TV and Mac App Store, may automatically download and install updates and content onto your device(s) or computer. You can turn off automatic updates altogether at any time by changing the automatic updates settings on your device or computer. To prevent the download of on-demand content within an App Store Product, delete the App Store Product from your device.

APP BUNDLES

Some App Store Products may contain multiple items (“App Bundles”). The price displayed with an App Bundle is the price you will be charged upon purchasing the App Bundle. The App Bundle price may be reduced to account for App Store Products you have already purchased or acquired, but may include a minimum charge to complete the App Bundle.

PRIVACY

The App and Book Services are subject to Apple's Privacy Policy at http://www.apple.com/legal/privacy/.

USE OF APP AND BOOK PRODUCTS AND THE APP AND BOOK SERVICES

You agree that the App and Book Services and certain App and Book Products include security technology that limits your use of App and Book Products and that, whether or not App and Book Products are limited by security technology, you shall use App and Book Products in compliance with the applicable usage rules established by Apple and its principals (“Usage Rules”), and that any other use of the App and Book Products may constitute a copyright infringement. Any security technology is an inseparable part of the App and Book Products. Apple reserves the right to modify the Usage Rules at any time. You agree not to violate, circumvent, reverse-engineer, decompile, disassemble, or otherwise tamper with any of the security technology related to such Usage Rules for any reason—or to attempt or assist another person to do so. Usage Rules may be controlled and monitored by Apple for compliance purposes, and Apple reserves the right to enforce the Usage Rules without notice to you. You agree not to access the App and Book Services by any means other than through software that is provided by Apple for accessing the App and Book Services. You shall not access or attempt to access an Account that you are not authorized to access. You agree not to modify the software in any manner or form, or to use modified versions of the software, for any purposes including obtaining unauthorized access to the App and Book Services. Violations of system or network security may result in civil or criminal liability.

The delivery of App and Book Products does not transfer to you any promotional use rights in the App and Book Products.

You acknowledge that, because some aspects of the App and Book Services, App and Book Products, and administration of the Usage Rules entails the ongoing involvement of Apple, if Apple changes any part of or discontinues the App and Book Services, which Apple may do at its election, you may not be able to use App and Book Products to the same extent as prior to such change or discontinuation, and that Apple shall have no liability to you in such case.

SUBMISSIONS TO THE APP AND BOOK SERVICES

The App and Book Services may offer interactive features that allow you to submit materials (including links to third-party content) on areas of the App and Book Services accessible and viewable by other users of the App and Book Services and the public. You agree that any use by you of such features, including any materials submitted by you, shall be your sole responsibility, shall not infringe or violate the rights of any other party or violate any laws, contribute to or encourage infringing or otherwise unlawful conduct, or otherwise be obscene, objectionable, or in poor taste. You also agree that you have obtained all necessary rights and licenses. You agree to provide accurate and complete information in connection with your submission of any materials on the App and Book Services. You hereby grant Apple a worldwide, royalty-free, nonexclusive license to use such materials as part of the App and Book Services or in relation to App and Book Products, without any compensation or obligation to you. Apple reserves the right to not post or publish any materials, and to remove or edit any material, at any time in its sole discretion without notice or liability. You may not submit reviews or ratings for App Store Products downloaded using a promotional Content Code.

Apple has the right, but not the obligation, to monitor any materials submitted by you or otherwise available on the App and Book Services, to investigate any reported or apparent violation of this Agreement, and to take any action that Apple in its sole discretion deems appropriate, including, without limitation, termination hereunder or under Apple's Copyright Policy (http://www.apple.com/legal/copyright.html).

THIRD-PARTY MATERIALS

Certain content, App and Book Products, and services available via the App and Book Services may include materials from third parties. Apple may provide links to third-party websites as a convenience to you. You agree that Apple is not responsible for examining or evaluating the content or accuracy and Apple does not warrant and will not have any liability or responsibility for any third-party materials or websites, or for any other materials, products, or services of third parties. You agree that you will not use any third-party materials in a manner that would infringe or violate the rights of any other party and that Apple is not in any way responsible for any such use by you.

OBJECTIONABLE MATERIAL

You understand that by using the App and Book Services, you may encounter material that you may deem to be offensive, indecent, or objectionable, and that such content may or may not be identified as having explicit material. Nevertheless, you agree to use the App and Book Services at your sole risk and Apple shall have no liability to you for material that may be found to be offensive, indecent, or objectionable. App and Book Product types and descriptions are provided for convenience, and you agree that Apple does not guarantee their accuracy.

INTELLECTUAL PROPERTY

You agree that the App and Book Services, including but not limited to App and Book Products, graphics, user interface, audio clips, editorial content, and the scripts and software used to implement the App and Book Services, contain proprietary information and material that is owned by Apple and/or its principals, and is protected by applicable intellectual property and other laws, including but not limited to copyright. You agree that you will not use such proprietary information or materials in any way whatsoever except for use of the App and Book Services in compliance with this Agreement. No portion of the App and Book Services may be reproduced in any form or by any means, except as expressly permitted in these terms. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the App and Book Services in any manner, and you shall not exploit the App and Book Services in any unauthorized way whatsoever, including, but not limited to, by trespass or burdening network capacity.

Notwithstanding any other provision of this Agreement, Apple and its principals reserve the right to change, suspend, remove, or disable access to any App and Book Products, content, or other materials comprising a part of the App and Book Services at any time without notice. In no event will Apple be liable for making these changes. Apple may also impose limits on the use of or access to certain features or portions of the App and Book Services, in any case and without notice or liability.

All copyrights in and to the App and Book Services (including the compilation of content, postings, links to other Internet resources, and descriptions of those resources) and related software are owned by Apple and/or its principals, who reserve all their rights in law and equity. THE USE OF THE SOFTWARE OR ANY PART OF THE APP AND BOOK SERVICES, EXCEPT FOR USE OF THE APP AND BOOK SERVICES AS PERMITTED IN THIS AGREEMENT, IS STRICTLY PROHIBITED AND INFRINGES ON THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS AND MAY SUBJECT YOU TO CIVIL AND CRIMINAL PENALTIES, INCLUDING POSSIBLE MONETARY DAMAGES, FOR COPYRIGHT INFRINGEMENT.

Apple, the Apple logo, iTunes, App Store, and other Apple trademarks, service marks, graphics, and logos used in connection with the App and Book Services are trademarks or registered trademarks of Apple Inc. in the U.S. and/or other countries. Other trademarks, service marks, graphics, and logos used in connection with the App and Book Services may be the trademarks of their respective owners. You are granted no right or license with respect to any of the aforesaid trademarks and any use of such trademarks.

TERMINATION

If you fail, or Apple suspects that you have failed, to comply with any of the provisions of this Agreement, Apple, at its sole discretion, without notice to you may: (i) terminate this Agreement and/or your Account, and you will remain liable for all amounts due under your Account up to and including the date of termination; and/or (ii) terminate the license to the software; and/or (iii) preclude access to the App and Book Services (or any part thereof).

Apple reserves the right to modify, suspend, or discontinue the App and Book Services (or any part or content thereof) at any time with or without notice to you, and Apple will not be liable to you or to any third party should it exercise such rights.

DISCLAIMER OF WARRANTIES; LIABILITY LIMITATIONS

APPLE DOES NOT GUARANTEE, REPRESENT, OR WARRANT THAT YOUR USE OF THE APP AND BOOK SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, AND YOU AGREE THAT FROM TIME TO TIME APPLE MAY REMOVE THE APP AND BOOK SERVICES FOR INDEFINITE PERIODS OF TIME, OR CANCEL THE APP AND BOOK SERVICES AT ANY TIME, WITHOUT NOTICE TO YOU.

YOU EXPRESSLY AGREE THAT YOUR USE OF, OR INABILITY TO USE, THE APP AND BOOK SERVICES IS AT YOUR SOLE RISK. THE APP AND BOOK SERVICES AND ALL PRODUCTS AND APP AND BOOK SERVICES DELIVERED TO YOU THROUGH THE APP AND BOOK SERVICES ARE (EXCEPT AS EXPRESSLY STATED BY APPLE) PROVIDED "AS IS" AND "AS AVAILABLE" FOR YOUR USE, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, THE ABOVE EXCLUSION OF IMPLIED WARRANTIES MAY NOT APPLY TO YOU.

IN NO CASE SHALL APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS, OR LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM YOUR USE OF ANY OF THE APP AND BOOK SERVICES OR FOR ANY OTHER CLAIM RELATED IN ANY WAY TO YOUR USE OF THE APP AND BOOK SERVICES, INCLUDING, BUT NOT LIMITED TO, ANY ERRORS OR OMISSIONS IN ANY CONTENT, OR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT (OR PRODUCT) POSTED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE APP AND BOOK SERVICES, EVEN IF ADVISED OF THEIR POSSIBILITY. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR THE LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, APPLE'S LIABILITY SHALL BE LIMITED TO THE EXTENT PERMITTED BY LAW.

APPLE SHALL USE REASONABLE EFFORTS TO PROTECT INFORMATION SUBMITTED BY YOU IN CONNECTION WITH THE APP AND BOOK SERVICES, BUT YOU AGREE THAT YOUR SUBMISSION OF SUCH INFORMATION IS AT YOUR SOLE RISK, AND APPLE HEREBY DISCLAIMS ANY AND ALL LIABILITY TO YOU FOR ANY LOSS OR LIABILITY RELATING TO SUCH INFORMATION IN ANY WAY.

APPLE DOES NOT REPRESENT OR GUARANTEE THAT THE APP AND BOOK SERVICES WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND APPLE DISCLAIMS ANY LIABILITY RELATING THERETO. YOU SHALL BE RESPONSIBLE FOR BACKING UP YOUR OWN SYSTEM, INCLUDING ANY APP AND BOOK PRODUCTS PURCHASED OR ACQUIRED FROM THE APP AND BOOK SERVICES.

WAIVER AND INDEMNITY

BY USING THE APP AND BOOK SERVICES, YOU AGREE, TO THE EXTENT PERMITTED BY LAW, TO INDEMNIFY AND HOLD APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS, AND LICENSORS HARMLESS WITH RESPECT TO ANY CLAIMS ARISING OUT OF YOUR BREACH OF THIS AGREEMENT, YOUR USE OF THE APP AND BOOK SERVICES, OR ANY ACTION TAKEN BY APPLE AS PART OF ITS INVESTIGATION OF A SUSPECTED VIOLATION OF THIS AGREEMENT OR AS A RESULT OF ITS FINDING OR DECISION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS MEANS THAT YOU CANNOT SUE OR RECOVER ANY DAMAGES FROM APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS, AND LICENSORS AS A RESULT OF ITS DECISION TO REMOVE OR REFUSE TO PROCESS ANY INFORMATION OR CONTENT, TO WARN YOU, TO SUSPEND OR TERMINATE YOUR ACCESS TO THE APP AND BOOK SERVICES, OR TO TAKE ANY OTHER ACTION DURING THE INVESTIGATION OF A SUSPECTED VIOLATION OR AS A RESULT OF APPLE'S CONCLUSION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS WAIVER AND INDEMNITY PROVISION APPLIES TO ALL VIOLATIONS DESCRIBED IN OR CONTEMPLATED BY THIS AGREEMENT.

CHANGES

Apple reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on your use of the App and Book Services. Such modifications and additional terms and conditions will be effective immediately and incorporated into this Agreement. Your continued use of the App and Book Services will be deemed acceptance thereof.

MISCELLANEOUS

This Agreement constitutes the entire agreement between you and Apple and governs your use of the App and Book Services, superseding any prior agreements between you and Apple. You also may be subject to additional terms and conditions that may apply when you use affiliate services, certain App and Book Products, third-party content, or third-party software. If any part of this Agreement is held invalid or unenforceable, that portion shall be construed in a manner consistent with applicable law to reflect, as nearly as possible, the original intentions of the parties, and the remaining portions shall remain in full force and effect. Apple's failure to enforce any right or provisions in this Agreement will not constitute a waiver of such or any other provision. Apple will not be responsible for failures to fulfill any obligations due to causes beyond its control.

The App and Book Services are operated by Apple from its offices in the United States. You agree to comply with all local, state, federal, and national laws, statutes, ordinances, and regulations that apply to your use of the App and Book Services. All transactions on the App and Book Services are governed by California law, without giving effect to its conflict of law provisions. Your use of the App and Book Services may also be subject to other laws. You expressly agree that exclusive jurisdiction for any claim or dispute with Apple or relating in any way to your use of the App And Book Services resides in the courts in the State of California. Risk of loss and title for all electronically delivered transactions pass to the purchaser in California upon electronic transmission to the recipient. No Apple employee or agent has the authority to vary this Agreement.

Apple may notify you with respect to the App and Book Services by sending an email message to your Account email address or a letter via postal mail to your Account mailing address, or by posting on the App and Book Services. Notices shall become effective immediately.

Apple reserves the right to take steps Apple believes are reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement. You agree that Apple has the right, without liability to you, to disclose any Registration Data and/or Account information to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement (including but not limited to Apple's right to cooperate with any legal process relating to your use of the App and Book Services and/or App and Book Products, and/or a third-party claim that your use of the App and Book Services and/or App and Book Products is unlawful and/or infringes such third party's rights).

STATUTORY EXCEPTIONS FOR PUBLIC INSTITUTIONS

If you are a qualified public educational or government institution and any part of this Agreement, such as, by way of example, all or part of the indemnification section, is invalid or unenforceable against you because of applicable state or federal law, then that portion shall be deemed invalid or unenforceable, as the case may be, and instead construed in a manner most consistent with applicable governing law. If California law is precluded, this Agreement shall be construed under the laws of the state in which your public educational or government institution is located.

ADDITIONAL MAC APP STORE AND APP STORE TERMS AND CONDITIONS

LICENSE OF MAC APP STORE AND APP STORE PRODUCTS

The software products made available through the Mac App Store and App Store (collectively, the “App Store Products”) are licensed, not sold, to you. There are two (2) categories of App Store Products, as follows: (i) those App Store Products that have been developed, and are licensed to you, by Apple (“Apple Products”); and (ii) those App Store Products that have been developed, and are licensed to you, by a third-party developer (“Third-Party Products”). The category of a particular App Store Product (Apple Product or Third-Party Product) is identified on the Mac App Store application or App Store application.

Your license to each App Store Product is subject to the Licensed Application End User License Agreement set forth below, and you agree that such terms will apply unless the App Store Product is covered by a valid end user license agreement entered into between you and the licensor of that App Store Product (the “Application Provider”), in which case the Application Provider’s end user license agreement will apply to that App Store Product. The Application Provider reserves all rights in and to the App Store Product not expressly granted to you.

You acknowledge that the license to each Apple Product that you obtain through the App Store Services, as defined below, or you associate with your Account, is a binding agreement between you and Apple. You acknowledge that: you are acquiring the license to each Third-Party Product from the Application Provider; Apple is acting as agent for the Application Provider in providing each such Third-Party Product to you; and Apple is not a party to the license between you and the Application Provider with respect to that Third-Party Product. The Application Provider of each Third-Party Product is solely responsible for that Third-Party Product, the content therein, any warranties to the extent that such warranties have not been disclaimed, and any claims that you or any other party may have relating to that Third-Party Product.

You acknowledge and agree that Apple and its subsidiaries are third-party beneficiaries of the Licensed Application End User License Agreement or the Application Provider’s end user license agreement, as the case may be, for each Third-Party Product. You also agree that, upon your acceptance of the terms and conditions of the license to any such Third-Party Product, Apple will have the right (and will be deemed to have accepted the right) to enforce such license against you as a third-party beneficiary thereof.

IN-APP PURCHASES

Certain App Store Products may include functionality that enables you to receive additional services, or licenses to additional functionality or content for use within the App Store Product ("In App Purchases"). In App Purchases that are consumed during the use of the App Store Product (for example, virtual ammunition) cannot be transferred among devices; can be downloaded only once; and after being downloaded, cannot be replaced. Once a consumable In App Purchase is acquired and received by you, Apple shall be without liability to you in the event of any loss, destruction, or damage. All In App Purchases are deemed App Store Products, and In App Purchases received within Third-Party Products are deemed Third-Party Products, and treated as such, for purposes of these terms and conditions.

You must authenticate to acquire In-App Purchases separately from any authentication to obtain App Store Products by entering your password when prompted, but once you have authenticated to obtain an In-App Purchase, you will be able to acquire additional In-App Purchases for fifteen minutes without re-entering your password. You can turn off the ability to acquire In-App Purchases on your iOS Device by following the steps outlined at http://support.apple.com/kb/HT4213.

IN-APP SUBSCRIPTIONS

Certain App Store Products may include functionality that enables you to acquire content on a subscription basis ("In App Subscriptions"). Paid In App Subscriptions are non-refundable. In App Subscriptions will automatically renew for the applicable time period you have selected, and, where applicable, your Account will be charged no more than 24-hours prior to the expiration of the current In App Subscription period. You may cancel automatic renewal of paid In App Subscriptions by selecting Manage App Subscriptions in your Account and selecting the subscription you want to modify. In the event of a price increase, the In App Subscription may continue at the new price upon prior notice to you unless you have cancelled automatic renewal. You may cancel free In App Subscriptions by deleting the App Store Product from your device. Certain paid In App Subscriptions may offer a free trial period prior to charging your Account. If you decide you do not want to purchase the In App Subscription, turn off auto-renewal in your Account settings during the free trial period. Certain In App Subscriptions may be designated as magazine and newspaper products. You should review additional information about the magazine and newspaper subscription offer at the point of sale within the App Store Product. We may ask for your permission to provide the name, email address and zip code listed in your Account to the Application Provider of such magazine and newspaper subscriptions so that the Application Provider can send you marketing messages about its own products in accordance with its publicly posted privacy policy. Once the Application Provider has this information, it will be treated in accordance with the Application Provider's privacy policy. We encourage you to learn about the privacy practices of the Application Provider before agreeing to give it your personal information. For more information, please review the Application Provider's privacy policy or contact the Application Provider directly.

POPULAR NEAR ME

When you opt in to Popular Near Me via enabling Location Services, Apple will, from time to time, automatically collect information related to certain of your App Store Products, such as your time spent with each App Store Product and the number of times each App Store Product is launched. This information is stored anonymously and will not be associated with your name or Account. Apple will use this information, as well as other information, such as your App Store Product download history, to give personalized recommendations to you.

Apple may use this information and combine it with aggregated information from

other users who opt in to this feature, your iTunes Store purchase history data, your App Store download data, aggregated App Store Product download data from other users, and other information like customer ratings of App Store Products, to:

- Provide you with recommendations regarding App Store Products, media, and other products and services that you may wish to purchase, download, or use.

- Provide recommendations to other users.

At all times your information will be treated in accordance with Apple's Privacy Policy.

If you prefer that we do not collect and use information from your device or system in this manner, you should not enable Location Services or use Popular Near Me . You can opt out at any time by turning off Popular Near Me in the System Services menu of the Location Services settings on your device .

MAC APP STORE PRODUCT USAGE RULES

Except as otherwise set forth herein,

(i) If you are an individual acting in your personal capacity, you may download and use an application from the Mac App Store (“Mac App Store Product”) for personal, non-commercial use on any Apple-branded products running Mac OS X (“Mac Computer”) that you own or control.

(ii) If you are a commercial enterprise or educational institution, you may download a Mac App Store Product for use by either (a) a single individual on each of the Mac Computer(s) used by that individual that you own or control or (b) multiple individuals on a single shared Mac Computer that you own or control. For example, a single employee may use a Mac App Store Product on both the employee’s desktop Mac Computer and laptop Mac Computer, or multiple students may serially use a Mac App Store Product on a single Mac Computer located at a resource center or library. For the sake of clarity, each Mac Computer used serially by multiple users requires a separate license.

(iii) Use may require sign-in with the Apple ID used to download the Mac App Store Product from the Mac App Store. Mac App Store Products can be updated through the Mac App Store only.

APP STORE AND APP STORE FOR APPLE TV PRODUCT USAGE RULES

(i) If you are an individual acting in your personal capacity, you may download and sync an App Store Product for personal, noncommercial use on any iOS or tvOS Device you own or control.

(ii) If you are a commercial enterprise or educational institution, you may download and sync an App Store Product for use by either (a) a single individual on one or more iOS or tvOS Devices used by that individual that you own or control or (b) multiple individuals, on a single shared iOS or tvOS Device you own or control. For example, a single employee may use an App Store Product on both the employee's iPhone and iPad, or multiple students may serially use an App Store Product on a single iPad located at a resource center or library. For the sake of clarity, each iOS or tvOS Device used serially or collectively by multiple users requires a separate license.

(iii) You shall be able to store App Store Products from up to five different Accounts at a time on a compatible iOS or tvOS Device.

(iv) You shall be able to manually sync App Store Products from at least one iTunes-authorized device to iOS Devices that have manual sync mode, provided that the App Store Product is associated with an Account on the primary iTunes-authorized device, where the primary iTunes-authorized device is the one that was first synced with the iOS Device or the one that you subsequently designate as primary using the iTunes application.

IMPORTANT SAFETY INFORMATION

To avoid muscle, joint, or eye strain during video game play, you should always take frequent breaks from playing, and take a longer rest if you experience any soreness, fatigue, or discomfort. A very small percentage of people may experience seizures or blackouts when exposed to flashing lights or patterns, including while playing video games or watching videos. Symptoms may include dizziness, nausea, involuntary movements, loss of awareness, altered vision, tingling, numbness, or other discomforts. Consult a doctor before playing video games if you have ever suffered these or similar symptoms, and stop playing immediately and see a doctor if they occur during game play. Parents should monitor their children’s video game play for signs of symptoms.

MAC APP STORE AND APP STORE PRODUCT MAINTENANCE AND SUPPORT

Apple will be responsible for providing any maintenance and support services with respect to the Apple Products only, as specified in the Licensed Application End User License Agreement or the separate end user license agreement, as the case may be, or as required under applicable law. The Application Provider of any Third-Party Product will be solely responsible for providing maintenance and support services with respect to that Product, as specified in the Licensed Application End User License Agreement or the Application Provider end user license agreement, as the case may be, or as required under applicable law.

LICENSED APPLICATION END USER LICENSE AGREEMENT

The Mac App Store Products,App Store Products and App Store for Apple TV Products (collectively, “App Store Product(s)”) made available through the Mac App Store Service,App Store Service and App Store for Apple TV Service (collectively, “App Store Service(s)”) are licensed, not sold, to you. Your license to each App Store Product that you obtain through the App Store Services or associate with your Account is subject to your prior acceptance of this Licensed Application End User License Agreement (“Standard EULA”), and you agree that the terms of this Standard EULA will apply to each App Store Product that you license through the App Store Service, unless that App Store Product is covered by a valid end user license agreement between you and the Application Provider of that App Store Product, in which case the terms of that separate end user license agreement will govern. Your license to any Apple Product under this Standard EULA or separate end user license agreement is granted by Apple, and your license to any Third-Party Product under this Standard EULA or separate end user license agreement is granted by the Application Provider of that Third-Party Product. Any App

Store Product that is subject to the license granted under this Standard EULA is referred to herein as the "Licensed Application". The Application Provider or Apple as applicable ("Licensor") reserves all rights in and to the Licensed Application not expressly granted to you under this Standard EULA.

a. Scope of License: This license granted to you for the Licensed Application by Licensor is limited to a nontransferable license to use the Licensed Application on any Apple-branded products running iOS (including but not limited to iPad, iPhone, and iPod touch) ("iOS Devices"), Mac OS X ("Mac Computers"), Apple Watch, and Apple TV, as applicable (collectively, "Apple Device(s)") that you own or control and as permitted by the usage rules set forth in the Mac App Store, App Store and iBooks Store Terms and Conditions (the "Usage Rules"). This license does not allow you to use the Licensed Application on any Apple Device that you do not own or control, and except as provided in the Usage Rules, you may not distribute or make the Licensed Application available over a network where it could be used by multiple devices at the same time. You may not rent, lease, lend, sell, transfer redistribute, or sublicense the Licensed Application and, if you sell your Apple Device to a third party, you must remove the Licensed Application from the Apple Device before doing so. You may not copy (except as expressly permitted by this license and the Usage Rules), decompile, reverse-engineer, disassemble, attempt to derive the source code of, modify, or create derivative works of the Licensed Application, any updates, or any part thereof (except as and only to the extent that any foregoing restriction is prohibited by applicable law or to the extent as may be permitted by the licensing terms governing use of any open-sourced components included with the Licensed Application). Any attempt to do so is a violation of the rights of the Licensor and its licensors. If you breach this restriction, you may be subject to prosecution and damages.

The terms of this license will govern any upgrades provided by Licensor that replace and/or supplement the original Licensed Application, unless such upgrade is accompanied by a separate license in which case the terms of that license will govern.

b. Consent to Use of Data: You agree that Licensor may collect and use technical data and related information—including but not limited to technical information about your device, system and application software, and peripherals—that is gathered periodically to facilitate the provision of software updates, product support, and other services to you (if any) related to the Licensed Application. Licensor may use this information, as long as it is in a form that does not personally identify you, to improve its products or to provide services or technologies to you.

c. Termination. The license is effective until terminated by you or Licensor. Your rights under this license will terminate automatically without notice from the Licensor if you fail to comply with any term (s) of this license. Upon termination of the license, you shall cease all use of the Licensed Application and destroy all copies, full or partial, of the Licensed Application.

d. External Services; Third-Party Materials. The Licensed Application may enable access to Licensor's and/or third-party services and websites (collectively and individually, "External Services"). Use of the External Services requires Internet access and use of certain External Services requires you to accept additional terms. By using this software in connection with an iTunes Store account, you agree to the latest iTunes Store Terms and Conditions and Usage Rules, which you may access and review at http://www.apple.com/legal/internet-services/itunes/ww/.

You understand that by using any of the External Services, you may encounter content that may be deemed offensive, indecent, or objectionable, which content may or may not be identified as having explicit language, and that the results of any search or entering of a particular URL may automatically and unintentionally generate links or references to objectionable material. Nevertheless, you agree to use the External Services at your sole risk and that neither the Licensor nor its agents shall have any liability to you for content that may be found to be offensive, indecent, or objectionable.

Certain External Services may display, include or make available content, data, information, applications or materials from third parties ("Third Party Materials") or provide links to certain third party web sites. By using the External Services, you acknowledge and agree that neither the Licensor nor its agents is responsible for examining or evaluating the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect of such Third Party Materials or web sites. Neither the Licensor nor its agents warrant or endorse and does not assume and will not have any liability or responsibility to you or any other person for any third-party services, Third Party Materials or web sites, or for any other materials, products, or services of third parties. Third Party Materials and links to other web sites are provided solely as a convenience to you.

Financial information displayed by any External Services is for general informational purposes only and should not be relied upon as investment advice. Before executing any securities transaction based upon information obtained through the External Services, you should consult with a financial or securities professional who is legally qualified to give financial or securities advice in your country or region. Medical information displayed by any App Store Product or External Service is for general information purposes only and should not be relied upon for medical diagnostic or treatment advice except as directed by a doctor. You should consult with a medical professional before relying on medical information available in an App Store Product. Location data provided by any External Services is for basic navigational purposes only and is not intended to be relied upon in situations where precise location information is needed or where erroneous, inaccurate, time-delayed or incomplete location data may lead to death, personal injury, property or environmental damage. Neither the Licensor, nor its agents, nor any of its content providers guarantees the availability, accuracy, completeness, reliability, or timeliness of stock information, location data or any other data displayed by any External Services.

You agree that the External Services contain proprietary content, information and material that is owned by Licensor and/or its agents or licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright, and that you will not use such proprietary content, information or materials in any way whatsoever except for permitted use of the External Services or in any manner that is inconsistent with the terms of this Standard EULA or that infringes any intellectual property rights of a third party or Apple. No portion of the External Services may be reproduced in any form or by any means. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the External Services, in any manner, and you shall not exploit the External Services in any unauthorized way whatsoever, including but not limited to, using the External Services to transmit any computer viruses, worms, trojan horses or other malware, or by trespass or burdening network capacity. You further agree not to use the External Services in any manner to harass, abuse, stalk, threaten, defame or otherwise infringe or violate the rights of any other party, and that neither Licensor nor its agents is in any way responsible for any such use by you, nor for any harassing, threatening, defamatory, offensive, infringing or illegal messages or transmissions that you may receive as a result of using any of the External Services.

In addition, External Services and Third Party Materials that may be accessed from, displayed on or linked to from the Apple Devices are not available in all languages or in all countries or regions. Licensor makes no representation that such External Services and Materials are appropriate or available for use in any particular location. To the extent you choose to use or access such External Services and Materials, you do so at your own initiative and are responsible for compliance with any applicable laws, including but not limited to applicable local laws. Licensor reserves the right to change, suspend, remove, or disable access to any External Services at any time without notice. In no event will Licensor be liable for the removal of or disabling of access to any such External Services. Licensor may also impose limits on the use of or access to certain External Services, in any case and without notice or liability.

e. NO WARRANTY: YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE LICENSED APPLICATION IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE LICENSED APPLICATION AND ANY SERVICES PERFORMED OR PROVIDED BY THE LICENSED APPLICATION ARE PROVIDED "AS IS" AND “AS AVAILABLE”, WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND LICENSOR HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE LICENSED APPLICATION AND ANY SERVICES, EITHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND OF NONINFRINGEMENT OF THIRD-PARTY RIGHTS. LICENSOR DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE LICENSED APPLICATION, THAT THE FUNCTIONS CONTAINED IN OR SERVICES PERFORMED OR PROVIDED BY THE LICENSED APPLICATION WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE LICENSED APPLICATION OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE LICENSED APPLICATION OR SERVICES WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY LICENSOR OR ITS AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE LICENSED APPLICATION OR SERVICES PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

f. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL LICENSOR BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE LICENSED APPLICATION, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT, OR OTHERWISE) AND EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Licensor’s total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of fifty dollars ($50.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

g. You may not use or otherwise export or re-export the Licensed Application except as authorized by United States law and the laws of the jurisdiction in which the Licensed Application was obtained. In particular, but without limitation, the Licensed Application may not be exported or re-exported (a) into any U.S.-embargoed countries or (b) to anyone on the U.S. Treasury Department's Specially Designated Nationals List or the U.S. Department of Commerce Denied Persons List or Entity List. By using the Licensed Application, you represent and warrant that you are not located in any such country or on any such list. You also agree that you will not use these products for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture, or production of nuclear, missile, or chemical or biological weapons.

h. The Licensed Application and related documentation are "Commercial Items", as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

i. The laws of the State of California, excluding its conflicts of law rules, govern this license and your use of the Licensed Application. Your use of the Licensed Application may also be subject to other local, state, national, or international laws.

ADDITIONAL IBOOKS STORE TERMS AND CONDITIONS

PURCHASE OF IBOOKS STORE PRODUCTS

You acknowledge that you are purchasing the content made available through the iBooks Store Service (the “iBooks Store Products”) from the third-party provider of that iBooks Store Product (the “Publisher”); Apple is acting as agent for the Publisher in providing each such iBooks Store Product to you; Apple is not a party to the transaction between you and the Publisher with respect to that iBooks Store Product; and the Publisher of each iBooks Store Product reserves the right to enforce the terms of use relating to that iBooks Store Product. The Publisher of each iBooks Store Product is solely responsible for that iBooks Store Product, the content therein, any warranties to the extent that such warranties have not been disclaimed, and any claims that you or any other party may have relating to that iBooks Store Product or your use of that iBooks Store Product.

IBOOKS STORE PRODUCT USAGE RULES

(i) You shall be authorized to use the iBooks Store Products only for personal, noncommercial use.

(ii) You shall be able to store iBooks Store Products from up to five different Accounts at a time on certain iOS-based devices, such as an iPad, iPod touch, or iPhone.

(iii) You shall be able to store iBooks Store Products on five iTunes-authorized devices at any time.

(iv) The delivery of iBooks Store Products does not transfer to you any promotional use rights in the iBooks Store Products or any rights to burn the iBooks Store Products to disc.

(v) You shall be able to manually sync iBooks Store Products from at least one iTunes-authorized device to devices that have manual sync mode, provided that the iBooks Store Product is associated with an Account on the primary iTunes-authorized device, where the primary iTunes-authorized device is the one that was first synced with the device or the one that you subsequently designate as primary using iTunes.

D. APPLE MUSIC TERMS AND CONDITIONS

THIS LEGAL AGREEMENT BETWEEN YOU AND APPLE INC. ("APPLE") GOVERNS YOUR USE OF THE APPLE MUSIC SERVICE AND ANY FEATURES ACCESSIBLE THEREFROM (THE “APPLE MUSIC SERVICE”).

THE APPLE MUSIC SERVICE

Apple is the provider of the Apple Music Service, which permits you to access digital music and other content (“Apple Music Products") for end user use only under the terms and conditions set forth in this Agreement.

REQUIREMENTS FOR USE OF THE APPLE MUSIC SERVICE

The Apple Music Service is only available to individuals aged at least 13 years (or equivalent minimum age based on local law), unless your Apple ID was provided to you as a result of a request by an approved educational institution or established as part of the Family Sharing feature by your parent or guardian. Children under the age of majority should review this Agreement with their parent or guardian to ensure that the child and parent or legal guardian understand it. We do not knowingly collect, use or disclose personal information from children under 13, or equivalent minimum age in the relevant jurisdiction, without verifiable parental consent. Parents and guardians should also remind any minors that conversing with strangers on the Internet can be dangerous and take appropriate precautions to protect children, including monitoring their use of the Apple Music Service.

The Apple Music Service is available to you only in the United States, its territories, and possessions. You agree not to use or attempt to use the Apple Music Service from outside these locations. Apple may use technologies to verify your compliance.

Use of the Apple Music Service requires a compatible device, Internet access, and certain software; may require periodic updates; and may be affected by the performance of these factors. High-speed Internet access is strongly recommended for regular use and is required for video; access or cellular data fees may apply. Requires iOS 8.4, iTunes 12.2 or Android 4.1 or later. The latest version of required software is recommended and may be required for certain transactions or features. You agree that meeting these requirements, which may change from time to time, is your responsibility.

YOUR APPLE MUSIC ACCOUNT

As a registered user of the Apple Music Service, you may establish an Account as set forth in, and subject to the terms of, the “Your Account” paragraph of the iTunes Store Terms and Conditions. In order to use some features of the Apple Music Service, you must enter your Apple ID and password or use Touch ID to authenticate your Account. You agree to provide accurate and complete iTunes Registration Data when you register with, and as you use, the Apple Music Service.

Apple logs information about your use of the Apple Music Service. This information includes, but is not limited to, the Apple Music Products you listen to (including whether you skip or stop) and the length of your listening session. Apple may also collect device information such as IP address, device type, operating system version and type, and unique device identifiers. Any music preference information you provide to Apple will also be stored in association with your Account. This information will be used by Apple for purposes such as providing the Apple Music Service, personalizing our recommendations to you, reporting to licensors and paying royalties, customizing and improving Apple products and Services including the Apple Music Service, providing relevant advertising, protecting against fraud and enforcing this Agreement.

By using the Apple Music Service, you agree and consent to Apple’s and its subsidiaries’ and agents’ transmission, collection, maintenance, processing, and use of this information for the aforementioned purposes and as otherwise permitted in accordance with Apple’s Privacy Policy, available here: http://www.apple.com/legal/privacy/.

APPLE MUSIC SUBSCRIPTION

If you buy a subscription to the Apple Music Service (an “Apple Music Subscription”), Apple will automatically charge the payment method associated with your Apple ID or the payment method associated with your Family Sharing Organizer’s account on a recurring basis until you turn off automatic renewal. You may turn off automatic renewal of your Apple Music Subscription at any time in the Account Settings menu on your device or computer, or in the Settings app on your device. If you turn off automatic renewal, you will continue to have access to the Apple Music Service for the remainder of your Apple Music Subscription term. When your Apple Music Subscription term ends, you will lose access to any feature of the Apple Music Service that requires an Apple Music Subscription, including but not limited to access to Apple Music Products accessible through the Apple Music Service or stored on your device, and any songs stored in your iCloud Music Library. Apple Music Subscription purchases are final. Your payment method will be charged no more than 24 hours prior to the expiration of the current Apple Music Subscription period.

To be eligible for an Apple Music Subscription at the family rate (where available), you must be enrolled in Family Sharing. If you are a Family Organizer, you agree that Apple will automatically charge your payment method on a recurring basis for any Apple Music Subscription purchases initiated by your Family members until automatic renewal is turned off on the applicable Family member’s device or computer.

YOU ARE RESPONSIBLE FOR THE TIMELY PAYMENT OF ALL APPLE MUSIC SUBSCRIPTION FEES AND FOR PROVIDING APPLE WITH A VALID PAYMENT METHOD. If Apple is unable to successfully charge your payment method for Apple Music Subscription fees due, Apple reserves the right to cancel your Apple Music Subscription. If your Apple Music Subscription is cancelled, you will lose access to any feature of the Apple Music Service that requires an Apple Music Subscription.

If you want to designate a different payment method or if there is a change in your payment method status, you must change your information in the Account Settings menu on your device or computer; this may temporarily disrupt your access to the Apple Music Service while Apple verifies your new payment information.

We may contact you via email or push notification regarding your Account or any Apple Music Service feature, for reasons including, without limitation, that your Apple Music Subscription will not automatically renew or will be cancelled.

Where available, you may be offered an Apple Music Subscription through your carrier (a "Carrier Subscription"). If you purchase a Carrier Subscription, your carrier will bill you for the cost of your Apple Music Subscription. Your relationship with the carrier is governed by the carrier's terms and conditions, not this Agreement, and any disputes related to a Carrier Subscription must be directed to your carrier, not Apple. By using the Apple Music Service, you agree that your carrier may exchange your carrier account information, telephone number and subscription information with Apple, and Apple may use this information to determine the status of your Carrier Subscription.

ICLOUD MUSIC LIBRARY

The iCloud Music Library feature is available to Apple Music subscribers who log in with an Apple ID. iCloud Music Library stores and permits you to remotely access songs and music videos purchased from the iTunes Store and other songs, along with related metadata, playlists, and other information from your other Apple Music-enabled devices. iCloud Music Library is turned on automatically when you set up your Apple Music Subscription. You will be prompted to enable iCloud Music Library when you log in to Apple Music on additional devices. You can enable iCloud Music Library in the Apple Music app settings on your device and in iTunes General Preferences on your computer. You can store up to 100,000 songs in iCloud Music Library. Songs purchased from the iTunes Store do not count against this limit. Songs that do not meet certain criteria or that are not authorized for your device or computer are not eligible for iCloud Music Library. You will not be able to access content stored in your iCloud Music Library when your Apple Music Subscription ends, but you can download songs that were previously acquired from the iTunes Store as set forth in, and subject to the terms of, the "Automatic Delivery and Downloading Previous Purchases" paragraph of the iTunes Store Terms and Conditions. You hereby agree to use iCloud Music Library only for lawfully acquired content. Any use for illegitimate content infringes the rights of others and may subject you to civil and criminal penalties, including possible monetary damages, for copyright infringement.

When you set up your Apple Music Subscription or enable iCloud Music Library, Apple Music will scan the song files on your device or computer and collect other information that may be used to identify media in your Music Library, such as the names of songs, song artists or song durations. iCloud Music Library will use this information to identify songs currently available on Apple Music, and will make identified songs available to you in a format then available on Apple Music. Unidentified songs on your device will remain in local storage, and unidentified songs on your computer are uploaded to iCloud Music Library in the same format or a format determined by Apple. You should backup your Music Library before setting up your Apple Music Subscription or enabling iCloud Music Library. Apple assumes no liability for content that is lost in connection with iCloud Music Library. iCloud Music Library should not be used as backup storage for content. Apple reserves the right to limit types of content uploaded (for example, excessively large files). Identified or uploaded songs and related metadata will be available for access from an Apple Music-compatible device into which you have logged in with your Account and that has been enabled for iCloud Music Library.

When you set up your Apple Music Subscription or enable iCloud Music Library, Apple logs information such as the tracks you play, stop or skip, the devices you use, and the time and duration of playback. By using iCloud Music Library, you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this information, including your iCloud Music Library usage information, to report to licensors and pay royalties, provide and improve Apple Music features and services and other Apple products and services, and as otherwise permitted in accordance with Apple's Privacy Policy, available here: http://www.apple.com/legal/privacy/.

SUBMISSIONS TO THE APPLE MUSIC SERVICE

The Apple Music Service may offer interactive features that allow you to submit materials (including but not limited to your name, picture, content, information and third-party content) on areas of the Apple Music Service accessible and viewable by the public. You agree that any use by you of such features, including any materials submitted by you, shall be your sole responsibility, shall not infringe or violate the rights of any other party or violate any laws, contribute to or encourage infringing or otherwise unlawful conduct, or otherwise be obscene, objectionable, or in poor taste. You also agree that you have obtained all necessary rights and licenses applicable to such materials and their distribution. You agree to provide accurate and complete information in connection with your submission of any materials on the Apple Music Service. You hereby grant Apple a worldwide, royalty-free, nonexclusive license to use such materials as part of the Apple Music Service or in relation to Apple Music Products, and the marketing of the Apple Music Service, without any compensation or obligation to you. Apple reserves the right to not post or publish any materials, and to remove or edit any material, at any time in its sole discretion without notice or liability.

Apple has the right, but not the obligation, to monitor any materials submitted by you or otherwise available on the Apple Music Service, to investigate any reported or apparent violation of this Agreement, and to take any action that Apple in its sole discretion deems appropriate, including, without limitation, termination hereunder or under Apple's Copyright Policy (http://www.apple.com/legal/copyright.html).

APPLE MUSIC SUBMISSIONS GUIDELINES

Content submitted to the Apple Music Service is subject to the following guidelines (the "Guidelines"), which may be updated from time to time. If you see content submitted to the Apple Music Service that does not comply with these Guidelines, please use the Report a Concern feature.

You may not use the Apple Music Service to:

- post objectionable, offensive or harmful content, including but not limited to content that is unlawful, harassing, threatening, defamatory, libelous, abusive, violent, obscene, vulgar, invasive of another's privacy, hateful, racially or ethnically offensive, or otherwise objectionable;

- post personal, private or confidential information belonging to others, including but not limited to phone numbers, addresses, billing information or photos or videos taken or distributed without the subject's permission;

- request personal information from a minor;

- impersonate or misrepresent yourself as another person, artist, entity, another Apple Music user, an Apple employee, or a civic or government leader, or otherwise misrepresent your affiliation with a person or entity (Apple reserves the right at any time to reject, reclaim, modify or block any Apple ID, user name, user handle or other identifier which could be deemed to be an impersonation or misrepresentation of your identity, or a misappropriation of another person's name or identity, or for any other reason at Apple's sole discretion);

- engage in copyright or other intellectual property infringement (including posting content that you do not own or have permission to post), or disclose any trade secret or confidential information in violation of a confidentiality, employment, or nondisclosure agreement;

- post or transmit spam, including but not limited to unsolicited or unauthorized advertising, promotional materials, or informational announcements;

- plan or engage in any illegal activity.

CONTENT AVAILABILITY

Apple and its licensors reserve the right to change, suspend, remove, discontinue or disable access to the Apple Music Service and any Apple Music Products, content, or other materials comprising a part of the Apple Music Service at any time without notice. In no event will Apple be liable for making these changes. Apple may also impose limits on the use of or access to certain features or portions of the Apple Music Service, in any case and without notice or liability.

USE OF CONTENT

You agree that the Apple Music Service includes security technology that limits your use of Apple Music Products and that, whether or not Apple Music Products are limited by security technology, you shall use Apple Music Products in compliance with the applicable usage rules established by Apple and its licensors ("Apple Music Usage Rules"), and that any other use of the Apple Music Products may constitute a copyright infringement. Any security technology is an inseparable part of the Apple Music Products and the Apple Music Service. Apple reserves the right to modify the Apple Music Usage Rules at any time. You agree not to violate, circumvent, reverse-engineer, decompile, disassemble, or otherwise tamper with any of the security technology related to such Apple Music Usage Rules for any reason, or to attempt or assist another person to do so. Apple Music Usage Rules may be controlled and monitored by Apple for compliance purposes, and Apple reserves the right to enforce the Apple Music Usage Rules without notice to you. You agree not to access the Apple Music Service by any means other than through software that is provided by Apple for accessing the Apple Music Service. You shall not access or attempt to access an Account that you are not authorized to access. You agree not to modify the software in any manner or form, or to use modified versions of the software, for any purposes including obtaining unauthorized access to the Apple Music Service. Violations of system or network security may result in civil or criminal liability.

APPLE MUSIC USAGE RULES

- You shall be authorized to use the Apple Music Service and Apple Music Products only for personal, noncommercial use, except as otherwise authorized by Apple.

- You shall be authorized to use the Apple Music Service on ten devices associated with your Account, only five of which can be computers. An individual Apple Music Subscription allows you to stream Apple Music Products to a single device at a time; a family Apple Music Subscription allows you and your Family members to stream Apple Music Products to up to six devices at a time.

- You shall not be entitled to burn Apple Music Products.

- The delivery of the Apple Music Service or Apple Music Products does not transfer to you any commercial or promotional use rights in the Apple Music Service or Apple Music Products.

THIRD-PARTY MATERIALS

Certain Apple Music Products, content, and services available via the Apple Music Service may include materials from third parties. Apple may provide links to third-party websites, products or services as a convenience to you. You agree that Apple is not responsible for examining or evaluating the content or accuracy and Apple does not warrant and will not have any liability or responsibility for any third-party materials, websites, products or services. You agree that you will not use any third-party materials in a manner that would infringe or violate the rights of any other party and that Apple is not in any way responsible for any such use by you.

OBJECTIONABLE MATERIAL

You understand that by using the Apple Music Service, you may encounter material that you may deem to be offensive, indecent, or objectionable, and that such content may or may not be identified as having explicit material. You agree to use the Apple Music Service at your sole risk and Apple shall have no liability to you for material that may be found to be offensive, indecent, or objectionable. Apple Music Product types and descriptions are provided for convenience, and you agree that Apple does not guarantee their accuracy.

INTELLECTUAL PROPERTY

You agree that the Apple Music Service, including but not limited to Apple Music Products, graphics, user interface, audio, video, editorial content, and the scripts and software used to implement the Apple Music Service, contains proprietary information and material that is owned by Apple and/or its licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright. You agree that you will not use such proprietary information or materials in any way whatsoever except for use of the Apple Music Service in compliance with this Agreement. No portion of the Apple Music Service may be reproduced in any form or by any means, except as expressly permitted in these terms. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the Apple Music Service in any manner, and you shall not exploit the Apple Music Service in any unauthorized way whatsoever, including, but not limited to, by trespass or burdening network capacity.

All copyrights in and to the Apple Music Service (including the compilation of content, postings, links to other Internet resources, and descriptions of those resources) and related software are owned by Apple and/or its licensors, who reserve all their rights in law and equity. THE USE OF THE SOFTWARE OR ANY PART OF THE APPLE MUSIC SERVICE, EXCEPT FOR USE OF THE APPLE MUSIC SERVICE AS PERMITTED IN THIS AGREEMENT, IS STRICTLY PROHIBITED AND INFRINGES ON THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS AND MAY SUBJECT YOU TO CIVIL AND CRIMINAL PENALTIES, INCLUDING POSSIBLE MONETARY DAMAGES, FOR COPYRIGHT INFRINGEMENT.

As user of the Apple Music Service in good standing, you may be provided with limited access to download certain album cover art for music stored on a device. Such access is provided as an accommodation only, and Apple does not warrant, and will not have any liability or responsibility for, such album cover art or your use thereof. You may access album cover art only in connection with the Apple Music Service. Album cover art is provided for personal, noncommercial use only. You agree that you will not use album cover art in any manner that would infringe or violate this Agreement or the rights of any other party, and that Apple is not in any way responsible for any such use by you.

TERMINATION

If you fail, or Apple suspects that you have failed, to comply with any of the provisions of this Agreement, Apple, at its sole discretion, without notice to you, and without waiving your liability for all amounts due under your Account, may: (i) terminate this Agreement and/or your Account; and/or (ii) terminate the license to the software; and/or (iii) preclude access to the Apple Music Service (or any part thereof).

DISCLAIMER OF WARRANTIES; LIABILITY LIMITATION

APPLE DOES NOT GUARANTEE, REPRESENT, OR WARRANT THAT YOUR USE OF THE APPLE MUSIC SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE, AND YOU AGREE THAT FROM TIME TO TIME APPLE MAY REMOVE THE APPLE MUSIC SERVICE FOR INDEFINITE PERIODS OF TIME, OR CANCEL THE APPLE MUSIC SERVICE AT ANY TIME, WITHOUT NOTICE TO YOU.

YOU EXPRESSLY AGREE THAT YOUR USE OF, OR INABILITY TO USE, THE APPLE MUSIC SERVICE IS AT YOUR SOLE RISK. THE APPLE MUSIC SERVICE AND ALL PRODUCTS AND SERVICES DELIVERED TO YOU THROUGH THE APPLE MUSIC SERVICE ARE (EXCEPT AS EXPRESSLY STATED BY APPLE) PROVIDED "AS IS" AND "AS AVAILABLE" FOR YOUR USE, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR

PURPOSE, TITLE, AND NONINFRINGEMENT. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, THE ABOVE EXCLUSION OF IMPLIED WARRANTIES MAY NOT APPLY TO YOU.

IN NO CASE SHALL APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, OR LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM YOUR USE OF THE APPLE MUSIC SERVICE OR FOR ANY OTHER CLAIM RELATED IN ANY WAY TO YOUR USE OF THE APPLE MUSIC SERVICE, INCLUDING, BUT NOT LIMITED TO, ANY ERRORS OR OMISSIONS IN ANY CONTENT OR APPLE MUSIC PRODUCTS, OR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT OR APPLE MUSIC PRODUCTS POSTED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE VIA THE APPLE MUSIC SERVICE, EVEN IF ADVISED OF THEIR POSSIBILITY. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR THE LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES OR JURISDICTIONS, APPLE'S LIABILITY SHALL BE LIMITED TO THE EXTENT PERMITTED BY LAW.

APPLE SHALL USE REASONABLE EFFORTS TO PROTECT INFORMATION SUBMITTED BY YOU IN CONNECTION WITH THE APPLE MUSIC SERVICE, BUT YOU AGREE THAT YOUR SUBMISSION OF SUCH INFORMATION IS AT YOUR SOLE RISK, AND APPLE HEREBY DISCLAIMS ANY AND ALL LIABILITY TO YOU FOR ANY LOSS OR LIABILITY RELATING TO SUCH INFORMATION IN ANY WAY.

APPLE DOES NOT REPRESENT OR GUARANTEE THAT THE APPLE MUSIC SERVICE WILL BE FREE FROM LOSS, CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, OR OTHER SECURITY INTRUSION, AND APPLE DISCLAIMS ANY LIABILITY RELATING THERETO. YOU SHALL BE RESPONSIBLE FOR BACKING UP YOUR OWN SYSTEM BEFORE, DURING AND AFTER USING THE APPLE MUSIC SERVICE, INCLUDING ANY CONTENT OR DATA USED IN CONNECTION WITH OR ACQUIRED FROM THE APPLE MUSIC SERVICE.

WAIVER AND INDEMNITY

BY USING THE APPLE MUSIC SERVICE, YOU AGREE, TO THE EXTENT PERMITTED BY LAW, TO INDEMNIFY AND HOLD APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, AND LICENSORS HARMLESS WITH RESPECT TO ANY CLAIMS ARISING OUT OF YOUR BREACH OF THIS AGREEMENT, YOUR USE OF THE APPLE MUSIC SERVICE, OR ANY ACTION TAKEN BY APPLE AS PART OF ITS INVESTIGATION OF A SUSPECTED VIOLATION OF THIS AGREEMENT OR AS A RESULT OF ITS FINDING OR DECISION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS MEANS THAT YOU CANNOT SUE OR RECOVER ANY DAMAGES FROM APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, AND LICENSORS AS A RESULT OF ITS DECISION TO REMOVE OR REFUSE TO PROCESS ANY INFORMATION OR CONTENT, TO WARN YOU, TO SUSPEND OR TERMINATE YOUR ACCESS TO THE APPLE MUSIC SERVICE, OR TO TAKE ANY OTHER ACTION DURING THE INVESTIGATION OF A SUSPECTED VIOLATION OR AS A RESULT OF APPLE'S CONCLUSION THAT A VIOLATION OF THIS AGREEMENT HAS OCCURRED. THIS WAIVER AND INDEMNITY PROVISION APPLIES TO ALL VIOLATIONS DESCRIBED IN OR CONTEMPLATED BY THIS AGREEMENT.

CHANGES

Apple reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on your use of the Apple Music Service. Such modifications and additional terms and conditions will be effective immediately and incorporated into this Agreement. Your continued use of the Apple Music Service will be deemed acceptance thereof.

COPYRIGHT NOTICE

If you believe that any Apple Music Products or any other content available through the Apple Music Service infringes a copyright claimed by you, please contact Apple's Copyright Agent as described in our Copyright Policy at http://www.apple.com/legal/trademark/claimsofcopyright.html. Apple may, in its sole discretion, suspend and/or terminate Accounts of users that are found to be repeat infringers.

MISCELLANEOUS

This Agreement constitutes the entire agreement between you and Apple and governs your use of the Apple Music Service, superseding any prior agreements between you and Apple. You also may be subject to additional terms and conditions that may apply when you use affiliate services, third-party content, or third-party software. If any part of this Agreement is held invalid or unenforceable, that portion shall be construed in a manner consistent with applicable law to reflect, as nearly as possible, the original intentions of the parties, and the remaining portions shall remain in full force and effect. Apple's failure to enforce any right or provisions in this Agreement will not constitute a waiver of such or any other provision. Apple will not be responsible for failures to fulfill any obligations due to causes beyond its control.

The Apple Music Service is operated by Apple from its offices in the United States. You agree to comply with all local, state, federal, and national laws, statutes, ordinances, and regulations that apply to your use of the Apple Music Service. All transactions on the Apple Music Service are governed by California law, without giving effect to its conflict of law provisions. Your use of the Apple Music Service may also be subject to other laws. You expressly agree that exclusive jurisdiction for any claim or dispute with Apple or relating in any way to your use of the Apple Music Service resides in the courts in the State of California. Risk of loss and title for all electronically delivered transactions pass to the purchaser in California upon electronic transmission to the recipient. No Apple employee or agent has the authority to vary this Agreement.

Apple may notify you with respect to the Apple Music Service by sending you an email message, or a letter via postal mail to your Account mailing address, or by a posting on the Apple Music Service. Notices shall become effective immediately.

Apple reserves the right to take steps Apple believes are reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement. You agree that Apple has the right, without liability to you, to disclose any Account information to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement (including but not limited to Apple's right to cooperate with any legal process relating to your use of the Apple Music Service and/or Apple Music Products, and/or a third-party claim that your use of the Apple Music Service and/or Apple Music Products is unlawful and/or infringes such third party's rights).

Last Updated: October 21, 2015

Exhibit 5

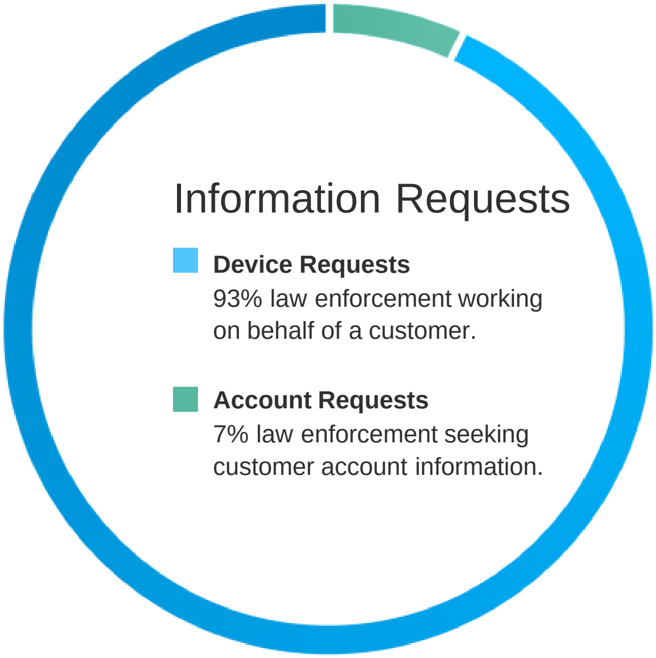
Our commitment to customer privacy doesn’t stop because of a government information request.

Government information requests are a consequence of doing business in the digital age. We believe in being as transparent as the law allows about what information is requested from us. In addition, Apple has never worked with any government agency from any country to create a “back door” in any of our products or services. We have also never allowed any government access to our servers. And we never will.

What we’re most commonly asked for and how we respond.

The most common requests we receive for information come from law enforcement in the form of either a Device Request or an Account Request. Our legal team carefully reviews each request, ensuring it is accompanied by valid legal process. All content requests require a search warrant. If we are legally compelled to divulge any information and it is not counterproductive to the facts of the case, we provide notice to the customer when allowed and deliver the narrowest set of information possible in response. National security-related requests are not considered Device Requests or Account Requests and are reported in a separate category altogether.

On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.



Device Requests

The vast majority of the requests Apple receives from law enforcement come from an agency working on behalf of a customer who has requested assistance locating a stolen device. We encourage any customer who suspects their device is stolen to contact their respective law enforcement agency.

Account Requests

Responding to an Account Request most often involves providing information about a customer’s iTunes or iCloud account. Only a small fraction of requests from law enforcement seek content such as email, photos, and other content stored on customers’ iCloud or iTunes accounts.

Read Apple’s transparency reports □

Read Apple's guidelines for law enforcement requests

US □ EMEIA □ Japan and APAC □

less than

0.00385%

of customers had data disclosed due to government information requests.

National Security Orders from the U.S. government.

A tiny percentage of our millions of accounts is affected by national security-related requests. In the first six months of 2014, we received 250 or fewer of these requests. Though we would like to be more specific, by law this is the most precise information we are currently allowed to disclose.

☆☆☆☆☆☆

from the Electronic Frontier Foundation

In its latest “Who Has Your Back?” report, the E.F.F. awarded Apple 6 out of 6 stars for our commitment to standing with our customers when the government seeks access to their data.

We’re working for greater transparency and protections on behalf of our customers.

We publish all request data permitted by law, but we believe our customers deserve to know more about what their governments and law enforcement agencies are requesting. We are actively engaged with the White House, as well as policymakers and government regulators around the world, to allow for more accurate and complete disclosures and reforms to overreaching surveillance laws and practices.

Supporting the fight for more accurate reporting

On November 5, 2013, Apple filed an *amicus curiae* motion in the U.S. Foreign Intelligence Surveillance Court. The motion requested that Apple and its competitors be allowed to publicly report more precise data on national security-related requests.

Read the full brief

Read the full letter included with the brief

Fighting against extraterritorial warrants

Apple filed an *amicus curiae* brief on June 13, 2014, challenging the notion that a U.S. search warrant requires a company to produce customer data stored outside the U.S. without government agencies adhering to the Mutual Legal Assistance Treaty process.

Read the full brief □

Apple filed an additional *amicus* brief on December 15, 2014 in the Second Circuit Court of Appeals further supporting its position that requiring a U.S. company to produce data about a non-U.S. citizen when the data is held by a foreign subsidiary and stored in a foreign location raises important conflicts of laws.

Read the full brief □

□ Privacy □ Government Information Requests

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Apple Info | Site Map | Hot News | RSS Feeds | Contact Us |

Terms of Use | Updated Privacy Policy |

Exhibit 6

IN THE

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NO. CA 78-2366

In the Matter of

THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING AN IN PROGRESS TRACE OF WIRE COMMUNICATIONS OVER TELEPHONE FACILITIES.

UNITED STATES OF AMERICA,

Plaintiff/Appellee,

vs.

MOUNTAIN STATES TELEPHONE & TELEGRAPH COMPANY,

Defendant/Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

BRIEF OF APPELLANT
THE MOUNTAIN STATES TELEPHONE & TELEGRAPH COMPANY

FENNEMORE, CRAIG, von AMMON & UDALL
A Professional Corporation
C. WEBB CROCKETT
GEORGE T. COLE
PATRICK WM. PATERSON
1700 First National Bank Plaza
100 West Washington Street
Phoenix, Arizona 85003
Attorneys for Appellant
The Mountain States Telephone
& Telegraph Company

IN THE

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

NO. CA 78-2366

In the Matter of

THE APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN ORDER
AUTHORIZING AN IN PROGRESS TRACE
OF WIRE COMMUNICATIONS OVER
TELEPHONE FACILITIES.

UNITED STATES OF AMERICA,

Plaintiff/Appellee,

vs.

MOUNTAIN STATES TELEPHONE & TELEGRAPH
COMPANY,

Defendant/Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

BRIEF OF APPELLANT
THE MOUNTAIN STATES TELEPHONE & TELEGRAPH COMPANY

FENNEMORE, CRAIG, von AMMON & UDALL
A Professional Corporation
C. WEBB CROCKETT
GEORGE T. COLE
PATRICK WM. PATERSON
1700 First National Bank Plaza
100 West Washington Street
Phoenix, Arizona 85003
Attorneys for Appellant
The Mountain States Telephone
& Telegraph Company

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES	Page
Basso v. Utah Power & Light Co., 495 F.2d 906 (10th Cir. 1974)	12
Berman v. Parker, 348 U.S. 26, 75 S. Ct. 98 (1954)	24
Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524 (1886)	15,16
Brittingham v. United States Com'r of Int. Rev., 451 F.2d 315 (5th Cir. 1971)	21
Chicot County Drainage Dist. v. Baxter State Bank, 308 U.S. 371, 60 S. Ct. 317, reh. denied, 309 U.S. 695, 60 S. Ct. 581 (1940)	20
Frank v. Maryland, 359 U.S. 360, 79 S. Ct. 804, reh. denied, 360 U.S. 914, 79 S. Ct. 1292 (1959), overruled on other grounds, Camara v. Municipal Court, 387 U.S. 523, 87 S. Ct. 1727 (1967)	16
Giles v. United States, 284 F. 208 (1st Cir. 1922)	17,18
Go-Bart Importing Co. v. United States, 282 U.S. 344, 51 S. Ct. 153 (1931)	14-15
Grace v. American Central Ins. Co., 109 U.S. 278, 3 S. Ct. 207 (1883)	11-12
Henry v. United States, 361 U.S. 98, 80 S. Ct. 168 (1959)	16
Jorden v. Metropolitan Utilities Dist., 498 F.2d 514 (8th Cir. 1974)	20-21
Lehigh Mining & Mfg. Co. v. Kelly, 160 U.S. 327, 16 S. Ct. 307 (1895)	11
Leonard v. United States, 6 F.2d 353 (1st Cir. 1925)	17

STATUTES

Federal Rules of Criminal Procedure, Rule 41	12
18 U.S.C. § 3105	23
28 U.S.C. § 1651(a)	20

OTHER AUTHORITIES

N. Lasson, The History and Development of the Fourth Amendment to the United States Constitution (1937)	15, 16-17

ISSUES PRESENTED

1. May a search warrant issued by a district court under the authority of Rule 41 of the Federal Rules of Criminal Procedure require a private party who is not a law enforcement agent to conduct a search?

2. Does the All Writs Act, 28 U.S.C. § 1651, authorize a district court to compel a telephone company to conduct a trace of incoming telephone calls?

3. Did the *ex parte* order entered against Mountain Bell in district court on May 26, 1978, requiring the company to trace incoming telephone calls deprive Mountain Bell of its property without due process of law in violation of the Fifth Amendment to the United States Constitution?

4. Did the order entered against Mountain Bell on May 26, 1978 in district court requiring Mountain Bell to trace incoming telephone calls constitute a taking of Mountain Bell's property without just compensation in violation of the Fifth Amendment to the United States Constitution?

PREFATORY NOTE

References made in this brief to the transcript of the hearing before the district court on June 5, 1978, will be designated "Tr.". References to the reporter's transcript of the record on appeal will be designated "R.".

STATEMENT OF THE CASE

This appeal arises out of an Order Authorizing the In-Progress Trace of Wire Communications ("Order") entered by the District Court for the District of Arizona which required The Mountain States Telephone and Telegraph Company ("Mountain Bell") to trace telephone calls to three specified telephone numbers located at a retail business establishment in Maricopa County, Arizona. The Order was obtained by the United States Attorney on Friday, May 26, 1978, with no prior notice having been given to Mountain Bell, and was served on Mountain Bell late in the afternoon of May 26. Although Mountain Bell opposed being required to conduct such a search on behalf of federal investigators, it promptly implemented the Order so that it would not be subject to contempt sanctions. Immediately after commencing the trace, however, Mountain Bell filed a motion to vacate asking the district court to set aside its _ex parte_ Order. The motion to vacate was denied on June 5, 1978 at the conclusion of a hearing on the matter.

Mountain Bell is now appealing both from the entry of the _ex parte_ Order requiring Mountain Bell to conduct a search of incoming phone calls and from the district court's refusal to grant the motion to vacate. A notice of appeal concerning both of these matters was filed June 14, 1978.

The United States Attorney began this proceeding by filing an Application with the district court asserting that probable cause existed to believe that specified telephone numbers were being used to violate the wagering tax provisions of federal law, 26 U.S.C. §§ 7201, 7203, and 7262. (R. 54) The Application requested an order "authorizing and directing the use of an electronic or mechanical device, which will record the telephone number or numbers of a dialing party when such party calls the known numbers. . . ." (R. 55) The Application further requested that the district court order Mountain Bell to "furnish the applicant forthwith all information, facilities, including, but not limited to, leased telephone lines and technical assistance necessary to accomplish this search. . . ." (R. 55) The Application gave no reason why such an order should be entered against Mountain Bell without first affording the company an opportunity to be heard.

As requested by the United States Attorney, the district court entered an order addressed to Special Agents of the Internal Revenue Service ("I.R.S.") and to Mountain Bell. (R. 61) The Order recited as authority that it was being entered "pursuant to Rule 41, Federal Rules of Criminal Procedure, and Title 28, United States Code, Section 1651(a)," the All Writs Act. (R. 62)

Although the United States Attorney sought the Order on behalf of the I.R.S. special agents and the Order was addressed to them, the I.R.S. special agents were not authorized or directed by the district court to conduct any part of the search. The Order placed the entire responsibility for the search on Mountain Bell, requiring that Mountain Bell "install and operate an electronic or mechanical device designed to trace and record the telephone number of a dialing party or parties when said party or parties call [the specified] telephone number" and further requiring that "all information gathered by reason of this Order be turned over to Special Agents of the Internal Revenue Service. . . ." (R. 62-63)

Mountain Bell was not able to present its arguments in opposition to the Order until June 5, 1978. Through memoranda of law filed with the district court in support of its motion to vacate, Mountain Bell asserted that neither Rule 41 nor the All Writs Act gave the district court authority to require the telephone company, against its will, to conduct a search on behalf of federal investigators. Through evidence presented at the June 5 hearing and case law submitted in its memoranda, Mountain Bell also demonstrated the burdens which the Order would impose upon it (R. 17-20; Tr. 19, 21, 24-25), and the differences between the tracing of incoming calls required in the present case and the identification of outgoing calls accomplished by law enforcement officials through the use of a pen register (R. 14-16).

To identify the numbers being called from a telephone under investigation, law enforcement officials conduct a search by means of a pen register. A "pen register" is a device attached to a given telephone line which records all numbers dialed on that line. The device detects changes in electrical currents, voltages or frequencies on the line which occur when the telephone is dialed. The pen register neither monitors or records any conversation which may take place on the line nor does it establish whether the call is actually completed. (R. 14, 15)

The actual connections, installation and operation of the pen register are done by the law enforcement agency itself, not the telephone company. (R. 14, 15) The pen register is installed by connecting it to the given telephone line at a point where the line makes an appearance in a terminal near the telephone under investigation. An "appearance" is the point at which the specific pair of wires serving the monitored telephone emerge from the sealed cable. When an appearance is not made at a terminal convenient for surveillance by the law enforcement officers, they can request and obtain a leased line from the telephone company. A "leased line" is an unused telephone line which makes an appearance in the same terminal as the monitored line. The leased line is cross-connected to the subject line. It is monitored at a more remote site where the pen register is connected. (R. 14, 15) Leased lines are provided by tariff and, like any tariff-prescribed service, are available to any subscriber who requests one. (R. 15) Such lines can permit two locations to be connected by a telephone line not necessarily passing through a telephone company central office. Business customers, for example, commonly use leased lines to provide direct inter-office communications.

In complying with a court order authorizing a pen register, the telephone company merely identifies the pair of wires providing service to the subject telephone line and, upon demand, provides a leased line pursuant to tariff. (R. 14, 15) In clear contrast, the Order on appeal here required Mountain Bell, rather than the I.R.S. agents, to conduct the search by installing and operating tracing equipment. Such equipment and services are not provided pursuant to tariffs and are not available to subscribers upon demand.

The Order entered in this case required the telephone company to trace calls in central offices employing "ESS" switching facilities. An "electronic switching system" ("ESS") office uses electronic switching equipment as distinguished from the mechanical devices or relays used in other switching systems. Such electronic switching is the most advanced system in use by Mountain Bell. Traces involving systems less advanced than an "ESS" would be even more complex, difficult and burdensome than the traces conducted under the Order in this case. (R. 15, Tr. 17)

In an "ESS" office, a trace may be initiated by programming the control computer in the "ESS" office to "trap" incoming calls to the designated telephone number. This programming is accomplished by use of a teletypewriter which permits a technician to communicate with the computer. (Tr. 19) When a call is made to the telephone number under surveillance, the "ESS" system identifies it as a call requiring unusual handling. The call is halted before the ringing cycle begins while the computer searches its memory to find the appropriate program to handle the call. Once the computer recognizes the call-trace program, it establishes the calling number, if possible, records this information in its memory for later print-out on the teletypewriter, and completes the call to the receiving telephone number. Altogether this process takes about two-and-one-half times the amount of computer processing time required for the completion of a routine call. (Tr. 20, 25.) Since the "ESS" computer has a finite amount of processing time, diverting time away from routine functions to the tracing of calls in an "ESS" office close to capacity could "bog the office down" or lead to a total central office failure. (Tr. 19, 21, 24-25.)

An "ESS" office can also be programmed to trap an outgoing call to a specified telephone number. When properly programmed it will record the number of a subscriber served by that office calling the specified number in another central office. To comply with the Order in this case all "ESS" offices in the Phoenix metropolitan area were programmed to trap outgoing and incoming calls to the subject numbers.

The equipment used to conduct a trace in an "ESS" office is the same equipment used to monitor and control the switching system. This includes the teletypewriter by which the computer communicates problems and malfunctions within the system to the supervising technician. Because the print-out generated by the trap of a telephone call to the subject number is routed to the teletypewriter on a priority basis, the technician will not be advised of these problems until after the traces have been reported. On traces requiring a heavy volume of calls to be trapped, traced and reported, the delay caused by call tracing could "mask" maintenance problems such that a potential problem diagnosed internally by the computer could develop into an actual malfunction or breakdown before the fact of its existence could be communicated through the teletypewriter to the technician. (Tr. 22, 23)

The tracing of a single call back to the calling number may involve several steps and require the participation of many different switching offices. In the simplest case where the subject call has originated within the same "ESS" office as the monitored telephone number, the tracing equipment would produce a print-out of the actual calling telephone number. However, if the call being traced originates in another central office, the tracing equipment will merely print out the designation of the "trunk line" over which the incoming call travelled into the receiving central office. Trunk lines are the cables connecting central offices. Some central offices which have a large interchange of traffic between them are connected by direct trunks. However, for less heavily used paths, trunk lines connect the individual central offices to a "tandem" office from which trunks then go out to other central offices or to other tandems to reach any desired central office.

The tracing of any particular call may involve three steps. First, from the monitored telephone number within the receiving central office to a tandem office (possibly in or out of the state); secondly, from that tandem office either to another tandem office or to the originating central office; and, lastly, within the originating central office to the telephone line of the calling party. The tracing of a call originating in another central office, especially one passing through one or more tandem offices, is not automatic. (R. 16) In fact, the process is most difficult and success is rarely achieved. (Tr. 10, 14) The Mountain Bell security supervisor summarized Mountain Bell's capability to trace calls as follows: "We have to be real lucky." (Tr. 14.)

ARGUMENT

This is a most difficult and very important case. Federal investigators obtained a court order authorizing an electronic search for incoming telephone calls to certain specified telephone numbers. However, the search was not to be performed by federal investigators. Instead, the district court's Order required an unwilling private citizen to conduct the search on behalf of federal investigators and to turn over the fruits of the search to them. The Order authorizing the search and requiring Mountain Bell to perform it was based upon a misconstruction of Rule 41 of the Federal Rules of Criminal Procedure and the All Writs Act. Since the two statutes will not support the Order, the search was conducted without statutory authority in violation of the Fourth Amendment to the United States Constitution. The Order also violated the Fifth Amendment to the United States Constitution because it permitted the government to take Mountain Bell's equipment and personnel and devote them to a public purpose with no prior opportunity to be heard and without providing appropriate compensation for the taking. The circumvention of the Fourth and Fifth Amendments which took place in this case cannot be permitted to stand.

Even though the Order which Mountain Bell is now appealing was fully complied with by the company and has now expired, this appeal has not been rendered moot. Searches are customarily confined to a somewhat limited time period which expires long before judicial review can take place. Hence, the constitutional and statutory violations which result from an order such as the one entered by the district court in this case are "capable of repetition, yet evading review." Roe v. Wade, 410 U.S. 113, 125, 93 S. Ct. 705, reh. denied, 410 U.S. 959, 93 S. Ct. 1409 (1973); Southern Pacific Terminal Co. v. Interstate Commerce Commission, 219 U.S. 498, 515, 31 S. Ct. 279 (1911). The United States Supreme Court recently applied this principle in United States v. New York Telephone Co., __ U.S. ___, 98 S. Ct. 364, 368 n. 6 (1977), to permit an appeal of an order entered against the New York Telephone Company under the authority of Rule 41 and the All Writs Act.

One of the reasons why this case is very difficult is that there is very little relevant authority beyond the actual text of the two statutes cited by the court in support of its order. The rule is well settled that a party seeking relief from a federal court must demonstrate that the case is within the jurisdiction and competence of that court. Because the presumption is that a federal court lacks jurisdiction or authority in a particular case absent an affirmative showing of such powers by the claimant, the government bears the burden of proof in invoking the jurisdiction of the district court. Lehigh Mining & Mfg. Co. v. Kelly, 160 U.S. 327, 16 S. Ct. 307 (1895); Grace v. American

Central Ins. Co., 109 U.S. 278, 3 S. Ct. 207 (1883); Basso v. Utah Power & Light Co., 495 F.2d 906 (10th Cir. 1974). Similarly, the burden of proof is placed upon the party seeking a court order and he is required to prove that the law supports his request. The procedure utilized by the government in the present case impermissibly reverses the customary placement of the burden of proof and requires Mountain Bell to disprove the lawfulness of the order sought by the government and the jurisdiction of the court. As a result, federal investigators may be permitted to conduct searches rather than prohibited from conducting them because of the scarceness of relevant authority.

The burden of proof which is normally imposed upon a government official requesting a search warrant is controlled by the requirement of the Fourth Amendment that "no Warrants shall Issue, but upon probable cause. . . ." Rule 41, too, requires the party seeking a search warrant to satisfy the court "that grounds for the application exist or that there is probable cause to believe that they exist. . . ." The Application submitted by the United States Attorney in this case addressed itself to the probable cause requirement and the Order entered by the court states that probable cause was found to exist. However, the United States Attorney should have carried an additional burden of proof. Because he was asking the district court to order Mountain Bell to conduct the search and to turn over the fruits of the search to special agents of the Internal Revenue Service, the United States Attorney should have been required to prove that such an Order directed to Mountain Bell was lawful and proper before the Order was entered. Nothing in the Application submitted by the United States Attorney or in the Order entered by the court indicates that the burden of proof on this issue was placed on the government or that the government brought forward evidence or legal authority sufficient to support its demand for an order compelling Mountain Bell to participate in the investigation.

Since Mountain Bell was not given notice of the application filed by the United States Attorney or given an opportunity to address the merits of the application before the Order compelling the company to participate in the investigation was entered by the court, the first opportunity Mountain Bell had to address these issues was in the motion which it filed asking the court to vacate its Order. By obtaining the Order through an ex parte application and forcing Mountain Bell to seek relief through a motion to vacate, the government effectively shifted the burden of proof to Mountain Bell on the question of whether Rule 41 and the All Writs Act authorized the Order entered against Mountain Bell. Moreover, Mountain Bell was thereby forced to overcome the natural inclination of any court to assume the validity of its orders unless error can be proven by the party seeking relief.

This appeal, again, places the burden on Mountain Bell to prove the invalidity of the Order entered against it by the district court. Such a burden is inequitable and should be lifted by this Court. Since the Order which is the subject of this appeal was obtained through an ex parte application containing no valid authority on the issue of the court's power to compel Mountain Bell to participate in the investigation, this Court should hold the Order to be unlawful unless the government can carry the burden which it should have had at the beginning of this case and prove that the Order is valid.

Mountain Bell's assertion that the government failed to comply with statutory requirements in obtaining a search warrant in this case is not an insignificant question of statutory construction. Statutes authorizing the issuance of search warrants permit the exercise of the state's investigatory powers against the public. Consequently, they should be strictly construed so as not to infringe upon the protections provided by the Fourth Amendment.

The constitutional limitations on the power of the state to conduct searches are established by the Fourth Amendment which guarantees the right of the people to be free from unreasonable searches. Go-Bart Importing Co. v.

United States, 282 U.S. 344, 357, 51 S. Ct. 153, 158 (1931). The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .

The protections afforded by the Fourth Amendment are designed not to permit criminals to escape discovery but, rather, to protect the general public from the unrestrained exercise of the investigatory powers of the state. The Supreme Court in Schmerber v. State of California, 384 U.S. 757, 767, 86 S. Ct. 1826, 1834 (1966), stated:

> "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."

The need to protect the individual citizen from the exercise of this power was one of the cornerstones of the American colonies' fight for independence from the English Crown. The Fourth Amendment was a specific response to a particular excess of the English government which the colonists found especially oppressive, namely, the writ of assistance. Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 87 S. Ct. 1642 (1967); Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524 (1886); N. Lasson. The History and Development of the Fourth Amendment to the United States Constitution (1937), 51-61.

Writs of assistance were general warrants authorizing the bearer to enter any house or any other place to search for and seize any prohibited foreign goods for which customs duties had not been paid. Such writs commanded all subjects of the Crown to assist in their execution. Writs of assistance have been cited as one of the principal catalysts of the American revolution and the importance of colonial resistance to these writs has frequently been emphasized by the Supreme Court. Frank v. Maryland, 359 U.S. 360, 363-365, 79 S. Ct. 804, 807-808, reh. denied, 360 U.S. 914, 79 S. Ct. 1292 (1959), overruled on other grounds, Camara v. Municipal Court, 387 U.S. 523, 87 S. Ct. 1727 (1967); Henry v. United States, 361 U.S. 98, 100-101, 80 S. Ct. 168, 170 (1959); Boyd v. United States, supra; N. Lasson, supra at 51-55.

Warrants permitting the exercise of unrestrained state search and seizure powers led directly to the creation of the Fourth Amendment and its guarantee of the fundamental right "to be secure . . . against unreasonable searches and seizures . . . ." Boyd v. United States, supra. A similar reaction was taking place in England at about the same time. The maxim that "a man's house is his castle" was eloquently expressed by William Pitt in an address before Parliament in 1766 as follows:

> The poorest man may, in his cottage, bid defiance to all the forces of the crown. It may be frail; its roof may shake; the

> wind may blow through it; the storm may
> enter; the rain may enter; but the King
> of England may not enter; all his force
> dares not cross the threshhold of the
> ruined tenement.
> (quoted in N. Lasson, supra at 49-50.)

The Fourth Amendment to the United States Constitution provides the protections described by William Pitt by prohibiting the state from exercising its search and seizure powers until after permission to exercise them has been obtained from a neutral magistrate. The magistrate's permission is granted in the form of a search warrant. Government investigators in the present case acknowledge that the law required them to obtain a search warrant and they sought such a warrant from the district court. However, statutes which authorize search warrants derogate the protections conferred by the Fourth Amendment and must be strictly construed. Leonard v. United States, 6 F.2d 353 (1st Cir. 1925); Giles v. United States, 284 F. 208 (1st Cir. 1922). The applicable statutes were not strictly construed in the present case.

From time to time since the adoption of the Fourth Amendment, Congress has found it appropriate in certain specific instances to permit the government to exercise its search powers. Without such a specific statutory grant of authority, the courts are powerless to issue search warrants. The Fourth Amendment itself requires compliance with strict procedures by providing "no warrants shall issue, . . . but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."

The statutes enacted by Congress have followed the constitutional mandate by imposing clearly specified procedures and requiring that they be followed. Rule 41, which was used as authority for the Order entered in this case, for example, requires that the warrant "be directed to a civil officer of the United States authorized to enforce or assist in enforcing any law thereof" and further requires the named officer "to search, within a specified period of time" and limits the search to "the person or place named for the property specified." A search which does not comply with the statutory warrant requirements is unreasonable. This requirement that a warrant strictly comply with the statutory requirements is a recognition that the power exercised by a government official in conducting a search is a "power capable of such oppressive and liberty destroying use that it should be strictly guarded and exercised." Giles v. United States, supra at 212. Moreover, the court in Giles stated with respect to the predecessor statute of Rule 41:

> "This careful codification of search warrant law leaves little or nothing for implication either as to the extent of the power or the method of its exercise."
> 284 F. at 212.

It is clear, then, that a warrant which is not specifically authorized by Rule 41, or another specific Congressional enactment, is invalid.

Rule 41 clearly does not authorize the district court to enter an order requiring Mountain Bell to conduct a search. The rule authorizes courts to permit specified law enforcement officials to exercise the inherent search and seizure powers possessed by the state. In effect, Rule 41 allows a court to remove temporarily the restraints on state power imposed by the Fourth Amendment. The rule does not empower a court to confer authority where it did not previously exist. To the extent that a search warrant is directed to anyone other than law enforcement officials, then, authority for the warrant must be found somewhere other than Rule 41. In the present case, law enforcement agents were not directed to conduct the search, nor did they conduct the search. Therefore, the Order cannot be supported by Rule 41.

The government apparently recognizes that Rule 41 does not authorize the district court to order a private citizen to conduct a search against his will on behalf of law enforcement officials. In its Application for a search warrant and in the order which it submitted to the court for entry, the government cited both Rule 41 and the All Writs Act as authority. The government's response to Mountain Bell's motion to vacate also cited the All Writs Act as the authority for requiring Mountain Bell to conduct the search for the government. Since Rule 41 provides no authority for an order directed to Mountain Bell, the Order entered by the district court against Mountain Bell must be reversed unless the government can establish that the All Writs Act confers power on the district court to order unwilling private citizens to conduct searches for the government. A review of the All Writs Act and other relevant authorities will show, however, that the government cannot meet this burden of proof.

The All Writs Act provides:

> (a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate <u>in aid of their respective jurisdictions</u> and agreeable to the usages and principles of law. [Emphasis added.]
>
> (b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction. 28 U.S.C.A. § 1651.

The All Writs Act and its statutory predecessors were enacted in order to provide the federal courts the power to issue orders concerning ministerial or collateral matters in support of jurisdiction conferred by other authority. It is fundamental that federal courts are courts of limited jurisdiction. <u>Chicot County Drainage Dist. v. Baxter State Bank</u>, 308 U.S. 371, 60 S. Ct. 317, <u>reh</u>. <u>denied</u>, 309 U.S. 695, 60 S. Ct. 581 (1940); <u>Jorden v. Metropolitan</u>

Utilities Dist., 498 F.2d 514 (8th Cir. 1974). They may act only when and in the manner expressly authorized by a congressional enactment. After federal courts were created by Congress, experience showed that they were having difficulties administering all of the details and collateral matters that were a part of cases within their admitted jurisdiction because they lacked the inherent powers possessed by common law courts. The All Writs Act is intended to fill in such jurisdictional gaps but only with respect to incidental or collateral matters. The All Writs Act does not in any manner expand the limited statutory jurisdiction of the federal courts nor provide the federal courts with an independent grant of jurisdiction. Rosenbaum v. Bauer, 120 U.S. 450, 7 S. Ct. 633 (1887); Brittingham v. United States Com'r of Int. Rev., 451 F.2d 315 (5th Cir. 1971); United States v. First Federal Sav. & Loan Ass'n, 248 F.2d 804 (7th Cir. 1957).

In the instant case, the jurisdiction of the district court is conferred by Rule 41. Under that Rule, the district court is given the power to permit federal law enforcement agents to conduct searches. Rule 41 does not give the district court power to compel private citizens to perform investigations for the government or power to take the property of private citizens and devote it to public purposes.

The All Writs Act simply cannot give the district court significant new jurisdiction which does not already exist under Rule 41. The Order entered against Mountain Bell in this case requiring it to devote its personnel and equipment to conducting a search on behalf of the government is not the exercise of judicial power over incidental or collateral matters. Such an order is the assertion of entirely new jurisdiction outside the bounds of Rule 41 and is not an order "in aid of [the court's] respective jurisdiction" under Rule 41 as required by the All Writs Act.

The misconstruction of the All Writs Act which took place in the present case is further demonstrated by the requirement that orders under the act be "agreeable to the usages and principles of law." In determining what auxiliary writs are "agreeable to the usages and principles of law," a court must first look to the common law. United States v. Hayman, 342 U.S. 205, 72 S. Ct. 263 (1952). None of the traditional common law writs authorizes a court to compel an unwilling third party to execute a search warrant in place of the authorized law enforcement officer. Even writs of assistance had been rejected in England by the time the American colonies declared their independence and their rejection of such writs is confirmed in the Fourth Amendment.

Further evidence that the All Writs Act does not authorize the Order entered against Mountain Bell in the present case is supplied by 18 U.S.C. § 3105. Rule 41(h) expressly provides that Rule 41 does not modify any other acts regulating searches and seizures. Section 3105 of 18 U.S.C. implicitly recognizes that the Fourth Amendment and Rule 41 permit searches only to be conducted by the law enforcement official named in the search warrant. Congress provided a very limited exception to the prohibition on searches by anyone other than the named official by enacting § 3105 which provides as follows:

> A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution. [Emphasis added.]

The search warrant granted by the district court in this case is addressed to special agents of the Internal Revenue Service and to Mountain Bell. Mountain Bell is not "an officer authorized by law to serve such warrant" or a government "officer" of any kind. Thus, a search by Mountain Bell is expressly prohibited by § 3105 since the special agents of the Internal Revenue Service were not "present" and were not "acting in [the warrant's] execution."

The district court's Order requiring Mountain Bell to conduct a search on behalf of the special agents of the Internal Revenue Service violates the Fifth Amendment to the United States Constitution as well as the Fourth Amendment. The Fifth Amendment provides that no private property shall "be taken for public use, without just compensation." The Fifth Amendment also provides that "no person" shall "be deprived of life, liberty, or property, without due process of law . . . ." The essence of due process is the requirement of a meaningful opportunity to be heard before the deprivation occurs. Since Mountain Bell's equipment and personnel were taken over for a public purpose without a prior hearing and without meaningful compensation, the district court's Order is unconstitutional and must be set aside.

There can be no doubt but that the expropriation of equipment and personnel for the purpose of conducting a criminal investigation is a taking for a public use. Berman v. Parker, 348 U.S. 26, 32, 75 S. Ct. 98, 102 (1954). The facts of this case make it manifest that just such an expropriation occurred.

The property which is taken from the telephone company in the operation of a trace includes the irreplaceable services provided by key personnel and the loss of use of various important pieces of equipment. The personnel required to operate a trace are skilled technicians who must be taken away from their regular duties monitoring, controlling and repairing the switching network. The services normally rendered by these personnel cannot later be made up when no longer needed by the trace operation. An extensive tracing on several subject telephones over a long period, such as 20 days, may involve tracing hundreds or thousands of calls and represents a significant drain on telephone company resources.

The dedication of personnel and equipment to tracing activities also significantly increases the likelihood of system malfunctions and breakdowns. For example, the computer which operates the system also diagnoses problems in the system which require maintenance or repair. The computer reports its discoveries to supervising technicians by printing out information on a teletypewriter. The same teletypewriter printer is used to report trace results. Since trace results are given priority over other matters on the printer, the supervising technician will not be notified of discovered problems until after trace results are reported. If Mountain Bell's technician is unable to communicate with the computer through the teletypewriter, a breakdown can occur which could have been prevented if the equipment were not involved in tracing calls for law enforcement officials.

A breakdown of Mountain Bell's equipment which could have been prevented if the supervising technician had been notified of the problem can result in lost revenue, lost opportunity costs, increased maintenance and administrative costs, and the replacement of equipment damaged by a system overload. All of such losses would be incurred by Mountain Bell as a direct result of the district court's Order.

The deprivation of Mountain Bell's property which was caused by the expropriation of the company's equipment and personnel for investigatory purposes violates the due process guarantees of the Fifth Amendment because the Order was entered and the investigation took place before Mountain Bell was afforded a hearing. The government obtained the Order requiring Mountain Bell to conduct a search through an ex parte application on Friday, May 26, 1978. The government did not notify Mountain Bell in advance of its intention to ask the district court to order the company to conduct the search. Neither the Application filed by the government nor the Order entered by the court contains any indication that notice to Mountain Bell could not reasonably have been given before the Order was considered.

Mountain Bell was likewise unable to test the validity of the Order after it was entered but before the taking actually occurred. The Order was served on Mountain Bell late Friday afternoon and the company was required to commence the search promptly in order to avoid being subject to contempt sanctions. By the time the court heard Mountain Bell's motion to vacate on June 5, 1978, the taking had already occurred. Such a hearing can provide no meaningful relief and cannot satisfy the due process requirements of the Fifth Amendment.

The Order at issue here also violates the Fifth Amendment's requirement that private property not be taken for a public use without just compensation. The just compensation required by the Constitution is "a full and perfect equivalent for the property taken." Monongahela Navigation Co. v. United States, 148 U.S. 312, 326, 13 S. Ct. 622, 626 (1893). It is the loss sustained by the owner of the property which measures just compensation, not the benefit derived by the government. The owner is to be compensated for all his losses, even where a market value cannot be readily calculated. United States v. Miller, 317 U.S. 369, 374, 63 S. Ct. 276, 280 (1943). The Order entered by the district court in this case does not meet these constitutional requirements.

Just compensation is denied to Mountain Bell by the district court's Order even though the order indicates that Mountain Bell should be reimbursed for its "expenses." The language of the Order provides as follows:

> That Mountain States Telephone and Telegraph Company be compensated and/or reimbursed for all charges and/or expenses at the prevailing rates for service or equipment furnished and/or expenses incurred in complying with this Order.

The compensation provisions of the Order do not appear to include compensation for the value of employee services lost to Mountain Bell, the value of preempted equipment, the costs of repair in the event that a trace causes equipment to break down or the revenues lost because of such a breakdown. The Order also does not appear to require compensation for any liability which Mountain Bell might incur because of conducting an electronic search on behalf of the government. It is not at all apparent that such "damages" are included within the concept of the "prevailing rates for services or equipment furnished and/or expenses incurred . . . ." If Mountain Bell is to receive just compensation to satisfy the requirements of the Fifth Amendment, either the Order or this Court should clearly provide for complete compensation of all damage suffered by Mountain Bell as a result of the expropriation of its personnel and facilities. In that regard, the Court should also clearly establish whether Mountain Bell is to be compensated for any liability which arises from its required participation in a search or seizure for the government or whether Mountain Bell is immune from such liability if it acts in compliance with the Order of a district court.

A review of the cases cited by the government in response to Mountain Bell's motion to vacate will demonstrate that the government has not carried its burden of proving that it is entitled to the Order which it received. The primary case relied upon by the government is the decision of the United States Supreme Court in _United States v. New York Telephone Co._, _supra_. However, the facts and the legal issues presented in that case are materially different from those presented in the present proceeding.

In _New York Telephone_, law enforcement officials wanted to install a pen register to record calls made from the telephone under surveillance. No trace of incoming calls was requested or at issue. To facilitate the installation of the pen register, the law enforcement officials requested that the telephone company provide a leased line to them so that they could install the pen register at a convenient site away from the point where the subject telephone line made an appearance. Leased lines are provided by telephone companies pursuant to tariffs and, like other tariff items, are available to any subscriber upon demand. The decision of the Supreme Court in _New York Telephone_ merely determined that a district court could require the telephone company to provide services or facilities authorized by tariffs. Since Mountain Bell's tariffs do not provide for tracing incoming telephone calls, Mountain Bell's subscribers are not entitled to such a service upon demand and Mountain Bell's refusal to provide such a service would not conflict with the company's tariffs. Such circumstances make the holding of _New York Telephone_ inapplicable to the present case.

The holding of New York Telephone is also inapplicable because of the substantial differences between the installation and operation of a pen register by law enforcement officials and the installation and operation of a trace by telephone company personnel. For a telephone company to comply with a court order authorizing a pen register such as was used in New York Telephone, the telephone company merely identifies the pair of wires providing service to the subject telephone. Law enforcement officials connect the pen register to the wires, operate the pen register and collect the information recorded by it. Law enforcement officials may also demand that the telephone company provide a leased line pursuant to tariff. Even when a leased line is provided, however, law enforcement officials install the pen register, operate it and collect the information recorded. The involvement of a telephone company in a search conducted by using a pen register is essentially none.

In contrast to the installation and operation of a pen register, a trace of incoming telephone calls is performed by telephone company personnel rather than law enforcement officials. The Order at issue in this case required Mountain Bell to program computers in various telephone company offices to identify calls coming into the subject numbers and attempt to trace the call back to its point of origination. The trace was performed by Mountain

Bell personnel using Mountain Bell equipment. Such a search cannot be compared to a search of outgoing calls by use of a pen register merely because both procedures constitute an electronic search of telephone communications.

Even the language used by the Supreme Court in its New York Telephone decision distinguishes that case from the Order entered in the present proceeding. In holding that the telephone company could not withhold its leased line services from law enforcement officials, the Supreme Court indicated that requiring such "meager assistance" of the telephone company did not exceed the limited jurisdiction possessed by the district court. Rather than merely identifying the location of the telephone lines under investigation and permitting law enforcement officials to conduct the search, the Order entered by the district court requires substantial involvement by Mountain Bell personnel and equipment. Since traces are handled on a priority basis, law enforcement officials obtain the use of Mountain Bell's personnel and equipment before Mountain Bell can use them in providing routine telecommunications services. Such a priority claim by the government can delay or prevent maintenance and repair work and can even cause failure of the system. Such conditions do not meet the requirements of New York Telephone.

The only other case cited by the government in support of its position opposing Mountain Bell's motion to vacate the Order was Michigan Bell Tel. Co. v. United States, 565 F.2d 385 (6th Cir. 1977). In that case, the court failed to discern the differences between law enforcement officials tracing outgoing telephone calls by means of a pen register and telephone company personnel tracing incoming telephone calls by means of electronic switching system computers. The court treated the two situations as indistinguishable because they both constituted electronic searches of telephone communications. Such an assumption is manifestly unwarranted and its inaccuracy is demonstrated by the facts of the present case. In affirming the trace order which a district court had directed to the telephone company, the Court of Appeals relied solely upon earlier cases involving pen registers. The court reasoned that a trace search of incoming calls could be ordered if other courts had previously ordered a pen register recording of outgoing telephone calls. The court's conlusion in that regard is unfounded and should be given no weight here.

Another reason why the Order should be set aside is that the procedure utilized by the government is fraught with the potential for abuse. The telephone communications network provided throughout the country by public service corporations such as Mountain Bell has great value to the public largely because it reaches into every home and office. Telephone company personnel regularly are admitted into the privacy of residences and offices to install, modify or repair telephone facilities. The successful accomplishment of the telephone company's function depends largely on continued freedom of access to such locations and continued public confidence that such employees are performing a public service. Orders such as the one entered by the district court greatly jeopardize such a relationship. In effect, the Order entered against Mountain Bell forces the company to become a part of the nation's law enforcement agencies. The telephone communications system in this country cannot continue to operate well if the public perceives telephone companies and their employees as law enforcement agents who may at any time be conducting unobtrusive searches.

If the present order is permitted to stand, where will the line be drawn? Will the government be permitted to demand the use of telephone company equipment such as vehicles, uniforms or identification badges? Will the government be permitted to require telephone company personnel to conduct searches as they visit residences and offices? Such risks must be avoided.

CONCLUSION

The Order of the district court and its denial of Mountain Bell's motion to vacate that Order should in all respects be declared unlawful and invalid.

Respectfully submitted this 23rd day of August, 1978.

FENNEMORE, CRAIG, von AMMON & UDALL
A Professional Corporation

By C. Webb Crockett
C. Webb Crockett
George T. Cole
Patrick Wm. Paterson
1700 First National Bank Plaza
100 West Washington Street
Phoenix, Arizona 85003
Attorneys for The Mountain States
Telephone & Telegraph Company

ADDENDUM

Fourth Amendment, United States Constitution

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Fifth Amendment, United States Constitution

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Rule 41, Federal Rules of Criminal Procedure

(a) Authority to Issue Warrant. A search warrant authorized by this rule may be issued by a federal magistrate or a judge of a state court of record within the district wherein the property sought is located, upon request of a federal law enforcement officer or an attorney for the government.

(b) Property Which May Be Seized with a Warrant. A warrant may be issued under this rule to search for and seize any (1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense.

(c) Issuance and Contents.

(1) Warrant upon affidavit. A warrant other than a warrant upon oral testimony under paragraph (2) of this subdivision shall issue only on an affidavit or affidavits sworn to before the federal magistrate or state judge and establishing the grounds for issuing the warrant. If the federal magistrate or state judge is satisfied that grounds for the application exist or that there is probable cause to believe that they exist, he shall issue a warrant identifying the property and naming or describing the person or place to be searched. The finding of probable cause may be based upon hearsay evidence in whole or in part. Before ruling on a request for a warrant the federal magistrate or state judge may

require the affiant to appear personally and may examine under oath the affiant and any witnesses he may produce, provided that such proceeding shall be taken down by a court reporter or recording equipment and made part of the affidavit. The warrant shall be directed to a civil officer of the United States authorized to enforce or assist in enforcing any law thereof or to a person so authorized by the President of the United States. It shall command the officer to search, within a specified period of time not to exceed 10 days, the person or place named for the property specified. The warrant shall be served in the daytime, unless the issuing authority, by appropriate provision in the warrant, and for reasonable cause shown, authorizes its execution at times other than daytime. It shall designate a federal magistrate to whom it shall be returned.

(2) Warrant upon oral testimony.

(A) General Rule.--If the circumstances make it reasonable to dispense with a written affidavit, a Federal Magistrate may issue a warrant based upon sworn oral testimony communicated by telephone or other appropriate means.

(B) Application.--The person who is requesting the warrant shall prepare a document to be known as a duplicate original warrant and shall read such duplicate original warrant, verbatim, to the Federal magistrate. The Federal magistrate shall enter, verbatim, what is so read to such magistrate on a document to be known as the original warrant. The federal magistrate may direct that the warrant be modified.

(C) Issuance.--If the Federal magistrate is satisfied that the circumstances are such as to make it reasonable to dispense with a written affidavit and that grounds for the application exist or that there is probable cause to believe that they exist, the Federal magistrate shall order the issuance of a warrant by directing the person requesting the warrant to sign the Federal magistrate's name on the duplicate original warrant. The Federal magistrate shall immediately sign the original warrant and enter on the face of the original warrant the exact time when the warrant was ordered to be issued. The finding of probable cause for a warrant upon oral testimony may be based on the same kind of evidence as is sufficient for a warrant upon affidavit.

(D) Recording and certification of testimony.--When a caller informs the Federal magistrate that the purpose of the call is to request a warrant, the Federal magistrate shall immediately place under oath each person whose testimony forms a basis of the application and each person applying for that warrant. If a voice recording device is available, the Federal magistrate shall record by means of such device all of the call after the caller informs the Federal magistrate that the purpose of the call is to request a warrant. Otherwise a stenographic or longhand verbatim record shall be made. If a voice recording device is used or a stenographic record made, the Federal magistrate shall have the record transcribed, shall certify the accuracy of the transcription, and shall file a copy of the original record and the transcription with the court. If a longhand verbatim record is made, the Federal magistrate shall file a signed copy with the court.

(E) Contents.--The contents of a warrant upon oral testimony shall be the same as the contents of a warrant upon affidavit.

(F) Additional rule for execution.--The person who executes the warrant shall enter the exact time of execution on the face of the duplicate original warrant.

(G) Motion to suppress precluded. --Absent a finding of bad faith, evidence obtained pursuant to a warrant issued under this paragraph is not subject to a motion to suppress on the ground that the circumstances were not such as to make it reasonable to dispense with a written affidavit.

(d) Execution and Return with Inventory. The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken. The inventory shall be made in the presence of the applicant for the warrant and the person from whose possession or premises the property was taken, if they are present, or in the presence of at least one credible person other than the applicant for the warrant or the person from whose possession or premises the property was taken, and shall be verified by the officer. The federal magistrate shall upon request deliver a copy of the inventory to the person from whom or from whose premises the property was taken and to the applicant for the warrant.

(e) Motion for Return of Property. A person aggrieved by an unlawful search and seizure may move the district court for the district in which the property was seized for the return of the property on the ground that he is entitled to lawful possession of the property which was illegally seized. The judge shall receive evidence on any issue of fact necessary to the decision of the motion. If the motion is granted the property shall be restored and it shall not be admissible in evidence at any hearing or trial. If a motion for return of property is made or comes on for hearing in the district of trial after an indictment or information is filed, it shall be treated also as a motion to suppress under Rule 12.

(f) Motion to Suppress. A motion to suppress evidence may be made in the court of the district of trial as provided in Rule 12.

(g) Return of Papers to Clerk. The federal magistrate before whom the warrant is returned shall attach to the warrant a copy of the return, inventory and all other papers in connection therewith and shall file them with the clerk of the district court for the district in which the property was seized.

(h) Scope and Definition. This rule does not modify any act, inconsistent with it, regulating search, seizure and the issuance and execution of search warrants in circumstances for which special provision is made. The term "property" is used in this rule to include documents, books, papers and any other tangible objects. The term "daytime" is used in this rule to mean the hours from 6:00 a.m. to 10:00 p.m. according to local time. The phrase "federal law enforcement officer" is used in this rule to mean any government agent, other than an attorney for the government as defined in Rule 54(c), who is engaged in the enforcement of the criminal laws and is within any category of officers authorized by the Attorney General to request the issuance of a search warrant.

18 U.S.C. § 3105

A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.

28 U.S.C. § 1651

(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on August 23, 1978, the original and twenty-five copies of the foregoing Brief of Appellant The Mountain States Telephone & Telegraph Company were mailed, certified mail, return receipt requested, postage prepaid to:

Hon. Emil E. Melfi, Jr.
Clerk, United States Court of
  Appeals for the Ninth Circuit
P. O. Box 547
San Francisco, CA 94101

and that on the same day, two copies of said Brief were mailed, postage prepaid, to the following person:

Michael D. Hawkins, United States Attorney
5000 Federal Building
230 North First Avenue
Phoenix, Arizona 85025
Attorney for Plaintiff/Appellee

C. Webb Crockett

C. Webb Crockett

Exhibit 7

The following table presents enacted fiscal year positions and expenditures for each agency area. These totals are comprised of State funds which include General Fund, special funds, and selected bond funds. These totals do not include federal funds, other non-governmental cost funds, or reimbursements.

State Agencies	2015-16				
	Positions	General Fund*	Special Funds*	Bond Funds*	Total State Funds*
K thru 12 Education	2,863.9	$49,373,454	$103,081	$1,063,236	$50,539,771
Higher Education	137,115.7	14,199,875	42,747	390,173	14,632,795
Health and Human Services	33,828.6	31,872,922	20,462,689	-	52,335,611
Corrections and Rehabilitation	61,528.0	10,077,743	2,578,288	-	12,656,031
Transportation	39,693.5	260,884	8,998,380	2,091,354	11,350,618
Natural Resources	19,944.1	2,481,304	1,303,960	1,097,486	4,882,750
Environmental Protection	5,810.7	71,514	2,721,463	1,492,056	4,285,033
Business, Consumer Services, Housing	5,674.0	626,778	807,492	139,685	1,573,955
Labor and Workforce Development	11,488.7	214,760	683,298	-	898,058
Government Operations	15,281.1	739,882	221,298	6,077	967,257
General Government	12,960.0	2,304,695	4,626,812	1,216	6,932,723
Legislative, Judicial, and Executive	17,547.7	3,145,729	3,167,679	206,540	6,519,948
TOTALS	**363,736.0**	**$115,369,540**	**$45,717,187**	**$6,487,823**	**$167,574,550**

* Dollars in thousands

Go to the **Enacted Budget Summary** web pages.

Exhibit 8

Report on Government Information Requests

January 1 - June 30, 2015

Apple takes our commitment to protecting your data very seriously and we work incredibly hard to deliver the most secure hardware, software and services available. We also believe every customer has a right to understand how their personal information is handled.

For government information requests, we report as much detail as we are legally allowed. When we receive an account request from law enforcement requesting a customer's personal information, we will notify the customer a request concerning their personal data was made unless we are explicitly prohibited from doing so. We are reserving the right to make exceptions, such as for extreme situations when we believe disclosing information could put a child or other person in serious danger, or where notice is not applicable to the underlying facts of the case.

Any government agency demanding customer content from Apple must get a search warrant. When we receive such a demand, our legal team carefully reviews it. If there's a question about the legitimacy or scope of the request we challenge it, as we have done as recently as this year. We only comply with information requests once we are satisfied that the request is valid and appropriate, and then we deliver the narrowest possible set of information.

How We Report Requests

The following tables detail account requests, device requests, emergency requests, National Security Orders, and requests for account deletion Apple received from January 1 through June 30, 2015.

Device Requests

Table 1 shows device requests. The vast majority of the requests we receive from law enforcement relate to information about lost or stolen devices, and we report these as device requests. Device requests may include requests for customer contact information provided to register a device with Apple or the date(s) the device used Apple services. We count devices based on the individual serial numbers related to an investigation. We encourage any customer who suspects their device is stolen to contact their local law enforcement agency.

Account Requests

Table 2 shows account requests. Responding to an account request usually involves providing information about an account holder's iTunes or iCloud account, such as a name and an address. In certain cases, we are asked to provide customers' iCloud content, which may include stored photos, email, iOS device backups, documents, contacts, calendars, and bookmarks. We consider these requests very carefully and provide account content when the legal request is a search warrant.

Emergency Requests

Table 3 shows all the emergency and/or exigent requests that we have received globally. Pursuant to 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4) Apple may voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay. The number of emergency requests that Apple deemed to be exigent and responded to is detailed in Table 3.

National Security Orders

Table 4 shows all the national security orders we have received, including orders received under FISA and National Security Letters (“NSLs”). To date, Apple has not received any orders for bulk data. We report all the national security orders we have received, including orders received under FISA and National Security Letters (“NSLs”), in bands of 250. Though we want to be more specific, this is currently the narrowest range allowed by the government.

Account Deletion Requests

Table 5 shows the number of account deletion requests we have received and how often we have complied with these demands.

Table 1: Device Requests January 1 - June 30, 2015

Country	Total Number of Law Enforcement Device Requests Received	Number of Devices Specified in the Requests	Number of Device Requests Where Some Data Was Provided	Percentage of Device Requests Where Some Data Was Provided
Latin America				
Brazil	26	437	22	85%
Panama	1	1	0	0%
Latin America Total	27	438	22	81%
Asia Pacific				
Australia	2986	4332	1777	60%
China	1129	4398	841	74%
Hong Kong	525	908	345	66%
Japan	234	488	136	58%
New Zealand	286	342	186	65%
Singapore	1712	2565	862	50%
South Korea	154	37565	85	55%
Taiwan	36	37	13	36%
Thailand	6	6	4	67%
Asia Pacific Total	7068	50641	4249	60%
USA				
United States of America	3824	9717	3093	81%
Canada				
Canada	25	134	17	68%

Table 1 (continued): Device Requests January 1 - June 30, 2015

Country	Total Number of Law Enforcement Device Requests Received	Number of Devices Specified in the Requests	Number of Device Requests Where Some Data Was Provided	Percentage of Device Requests Where Some Data Was Provided
Europe, Middle East, India, Africa				
Austria	98	219	60	61%
Belgium	84	242	42	50%
Burkina Faso	1	1	0	0%
Cyprus	1	1	1	100%
Czech Republic	25	11258	10	40%
Denmark	79	322	63	80%
Finland	15	53	10	67%
France	1432	16099	528	37%
Germany	9659	21809	5074	53%
Greece	10	18	8	80%
Hungary	25	447	12	48%
Iceland	3	4	2	67%
India	36	45	7	19%
Ireland	200	472	139	70%
Israel	4	12	4	100%
Italy	906	1291	584	64%
Latvia	2	2	0	0%
Lithuania	1	3	1	100%
Luxembourg	10	29	2	20%
Netherlands	25	85	12	48%
Norway	60	140	43	72%
Poland*	53	241509	28	53%
Portugal	64	106	35	55%
Romania	3	19	2	67%
Russia	30	72	7	23%
Serbia	2	2	0	0%
Slovenia	30	69	13	43%
South Africa	5	6	2	40%
Spain	1033	2074	652	63%
Sweden	166	393	108	65%
Switzerland	156	506	105	67%
Turkey	43	60	23	53%
United Kingdom	1791	4496	999	56%
Europe, Middle East, India, Africa Total	16052	301864	8576	53%

*Poland: predominately requests from Polish Customs and Revenue Authorities.

Table 2: Account Requests January 1 - June 30, 2015

Country	Total Number of Law Enforcement Account Requests Received	Number of Accounts Specified in the Requests	Number of Accounts for Which Data Was Disclosed	Number of Account Requests Where Apple Objected	Number of Account Requests Where No Data Was Disclosed	Number of Account Requests Where Non-Content Data Was Disclosed	Number of Account Requests Where Some Content Was Disclosed	Percentage of Account Requests Where Some Data Was Disclosed
Latin America								
Brazil	4	4	3	0	1	3	0	75%
Colombia	1	1	1	0	0	1	0	100%
Latin America Total	5	5	4	0	1	4	0	80%
Asia Pacific								
Australia	98	108	12	75	86	12	0	12%
China	24	85	9	14	17	7	0	29%
Hong Kong	14	50	44	3	3	11	0	79%
Japan	51	879	92	33	31	20	0	39%
New Zealand	4	4	1	2	3	1	0	25%
Singapore	26	41	16	14	17	9	0	35%
South Korea	17	57	33	10	10	7	0	41%
Taiwan	13	13	7	8	6	7	0	54%
Asia Pacific Total	247	1237	214	159	173	74	0	30%
USA								
United States of America	971	2727	1407	116	181	495	295	81%
Canada								
Canada	8	9	11	2	0	7	1	100%

Table 2 (continued): Account Requests January 1 - June 30, 2015

Country	Total Number of Law Enforcement Account Requests Received	Number of Accounts Specified in the Requests	Number of Accounts for Which Data Was Disclosed	Number of Account Requests Where Apple Objected	Number of Account Requests Where No Data Was Disclosed	Number of Account Requests Where Non-Content Data Was Disclosed	Number of Account Requests Where Some Content Was Disclosed	Percentage of Account Requests Where Some Data Was Disclosed
Europe, Middle East, India, Africa								
Austria	7	7	4	1	3	4	0	57%
Belarus	2	2	2	0	0	2	0	100%
Belgium	1	1	1	0	0	1	0	100%
Cyprus	2	2	1	1	1	1	0	50%
Denmark	3	3	1	0	2	1	0	33%
France	43	51	25	13	22	20	1	49%
Germany	78	91	33	29	45	33	0	42%
Greece	5	5	4	1	1	4	0	80%
Hungary	3	3	0	3	3	0	0	0%
India	1	1	0	0	1	0	0	0%
Ireland	4	4	0	1	4	0	0	0%
Italy	29	32	14	8	15	14	0	48%
Malta	2	2	2	0	0	2	0	100%
Netherlands	3	3	1	2	2	1	0	33%
Norway	3	5	4	0	1	2	0	67%
Pakistan	2	2	1	0	1	1	0	50%
Portugal	2	3	3	0	0	2	0	100%
Romania	1	1	0	1	1	0	0	0%
Russia	3	3	0	3	3	0	0	0%
Spain	19	24	12	5	9	10	0	53%
Sweden	5	5	1	1	4	1	0	20%
Switzerland	5	5	1	3	4	1	0	20%
Turkey	6	7	0	5	6	0	0	0%
United Kingdom	207	232	140	47	77	130	0	63%
Europe, Middle East, India, Africa Total	436	494	250	124	205	230	1	53%

Table 3: Emergency Requests January 1 - June 30, 2015

Country	Total Number of Emergency Requests Received
Latin America	
Brazil	2
Asia Pacific	
Japan	2
USA	
United States of America	107
Canada	
Canada	14
Europe, Middle East, India, Africa	
Austria	1
Belgium	1
France	7
Germany	1
Greece	1
Hungary	1
India	2
Ireland	1
Italy	2
Monaco	2
Netherlands	1
Spain	1
Sweden	2
United Kingdom	98
Total	246

Table 4: National Security Requests January 1 - June 30, 2015

	1/1/2015 - 6/30/2015
National Security Orders Received	750-999
Total Accounts Affected	250-499

Table 5: Account Deletion Requests by Government January 1 - June 30, 2015

(Court order or search warrant required)

Number of Account Deletion Requests Received	Number of Account Deletion Requests Where Apple Objected	Number of Account Deletion Requests Where Account Was Deleted*
1	0	0

*One account deletion request was received, to which Apple did not object; but there was no data in the specified account so it was not deleted.

Glossary of Terms

Table 1 Definitions

Total Number of Law Enforcement Device Requests Received

The number of device-based requests issued by a government agency and/or a court that are received by Apple and seek customer data related to specific device identifiers such as serial or IMEI numbers. Law enforcement device requests come in various forms such as subpoenas, court orders, and warrants. A single request may involve multiple devices. For example, in the case of a recovered shipment of stolen devices, law enforcement may seek information related to several devices in a single request.

Number of Devices Specified in the Requests

The total number of iPhone, iPad, iPod, Mac, or other devices identified in each law enforcement request, based on the number of device identifiers. For example, law enforcement agencies investigating theft cases often send requests seeking information based on serial numbers. Each serial number is counted as a single device. A request may involve multiple devices as in the case of a recovered shipment of stolen devices.

Number of Device Requests Where Some Data Was Provided

The number of law enforcement requests that resulted in Apple providing relevant device information, such as registration, subscriber, service, repair, and purchase information in response to valid legal process.

Percentage of Device Requests Where Some Data Was Provided

The percentage of law enforcement requests that resulted in Apple providing some relevant device information in response to valid legal process.

Table 2 Definitions

Total Number of Law Enforcement Account Requests Received

The total number of account-based requests issued by a government agency and/or a court that are received by Apple and seek customer data related to specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers. Account-based law enforcement requests come in various forms such as subpoenas, court orders, and warrants.

Number of Accounts Specified in the Requests

The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers in each law enforcement request. A single request may involve multiple accounts where, for example, multiple accounts are associated with the same credit card.

Number of Accounts for Which Data Was Disclosed

The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers, for which Apple provided some iCloud, iTunes, or Game Center data.

Number of Account Requests Where Apple Objected

The number of law enforcement requests that resulted in Apple refusing to provide some data based on various grounds, such as jurisdiction, improper process, insufficient process, invalid process, or where the scope of the request was excessively broad. For example, Apple may object to a law enforcement request as "invalid" if it were not signed.

Number of Account Requests Where No Data Was Disclosed

The number of law enforcement requests that resulted in Apple providing no customer information whatsoever.

Number of Account Requests Where Non-Content Data Was Disclosed

The number of law enforcement requests that resulted in Apple providing only subscriber or transactional information, but not content. For example, Apple may provide subscriber information and a limited purchase history in response to valid legal process.

Number of Account Requests Where Some Content Was Disclosed

The number of law enforcement requests where Apple determined that an account request was lawful and provided content such as iCloud email, contacts, calendar, or Photo Stream content. Apple only provides user account content in extremely limited circumstances.

Percentage of Account Requests Where Some Data Was Disclosed

The percentage of law enforcement requests that resulted in Apple providing some iCloud, iTunes, or Game Center data.

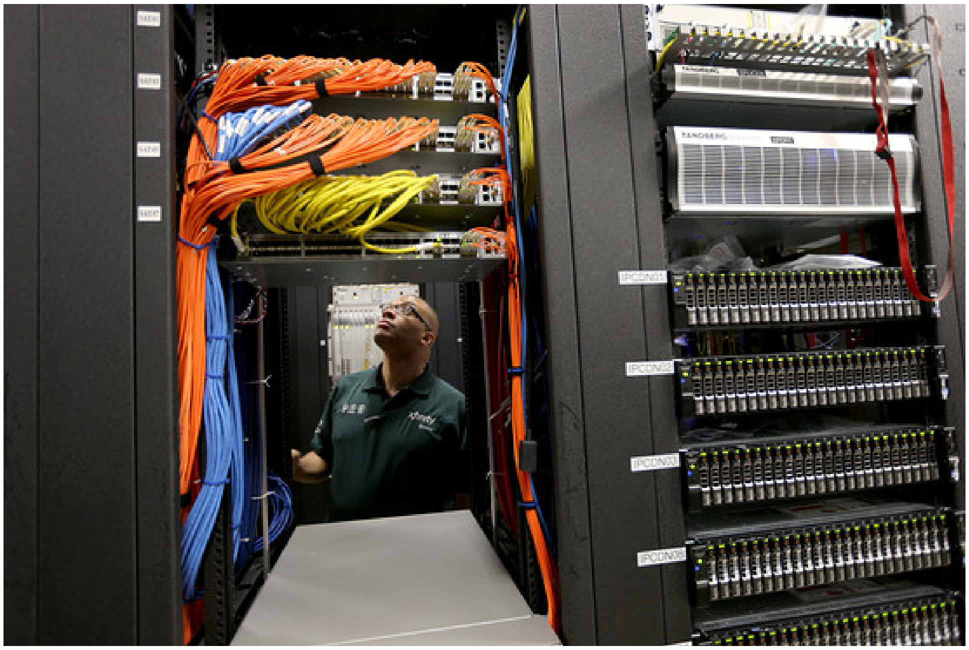
Exhibit 9

THE WALL STREET JOURNAL.
WSJ.com

August 15, 2014, 5:46 AM ET

Apple Adds State-Controlled China Telecom as Data Center Provider

ByLorraine Luk



Getty Images

In its latest effort to dispel security concerns raised by China, Apple has begun storing its users' data in China on state-controlled China Telecom's Internet-based storage.

But the company said Friday in a statement to The Wall Street Journal that all data stored is encrypted, meaning China Telecom won't have access to its content.

"Apple takes user security and privacy very seriously. We have added China Telecom to our list of data center providers to increase bandwidth and improve performance for our customers in mainland China," it said.

On a statement posted on the Fuzhou city government's website, China Telecom confirmed that Apple began storing user's iCloud data on China Telecom's platform on Aug. 8.

"After 15 months of stringent tests and evaluation… China Telecom has become Apple's only cloud service provider in China," a China Telecom's unit said in the statement.

Apple's iCloud is an Internet-based storage service used to back up data on all of its devices including iPhones and iPad. The service lets users access their music, photos, documents and more from whatever Apple device they are on.

Apple declined to comment on whether the deal with China Telecom was to dispel security concerns of the Chinese government.

Apple's collaboration with China Telecom comes after in July state-run China Central Television claimed the iPhone poses a "national security concern" because of a feature that learns the locations of places a user visits most frequently. In response, Apple pointed out that users must switch on that feature themselves and the company doesn't keep track of the location.

Gartner analyst Sandy Shen said the deal with China Telecom would alleviate the Chinese government's concerns about potential leak of user information.

"China always requires Chinese banks and local telecom operators to store their user data in the country for the purpose of national security. Apple storing its iCloud data in China would help to provide a better user experience as direct connection to the local server would allow faster and more stable access to iCloud services," said Shen.

China has been an attractive but challenging market for U.S. technology companies, especially when commercial and political tensions are escalating between the U.S. and China over cybersecurity concerns.

Last month, Chinese investigators raided Microsoft's offices in four Chinese cities as part of an anti-monopoly investigation. Qualcomm, a major supplier of cellphone chips, also has been under investigation since November over how it calculates patent-licensing and royalty rates in China and other issues.

Exhibit 10

Home (/) / Web Apps (/Category/Web-Apps/)

Apple Tweaks Wi-Fi in IPhone to Use China Protocol

COMMENTS

By Owen Fletcher (/au hor/Owen-Fletcher/), IDG News Service

Apple appears to have tweaked its iPhone to support a Chinese security protocol for wireless networks, as companies increasingly adopt Chinese government-backed technologies to break into the country's huge market.

The move suggests Apple may soon launch a new version of the iPhone in China with Wi-Fi, a feature that regulations previously barred.

Chinese regulators last month approved the frequency ranges used by a new Apple mobile phone with 3G and wireless LAN support, the Web site of China's State Radio Monitoring Center (http://www.srrc.org.cn/WP_Search.aspx) shows. The device appears to be an iPhone and uses GSM and the 3G standard WCDMA, just like iPhones currently offered in China by local carrier China Unicom.

Apple removed Wi-Fi on the iPhones now sold in China because regulators there began approving mobile phones with WLAN support only last year -- and only if they supported a homegrown Chinese security protocol called WAPI (WLAN Authentication and Privacy Infrastructure).

The new Apple phone does support WAPI, according to the Chinese regulatory site. If an iPhone with WAPI goes on sale, Apple would be one of the highest-profile companies to offer a device using the protocol.

The new Apple phone may also support standard Wi-Fi. The Chinese security protocol is an alternative for just part of Wi-Fi, and devices can support both it and the technology it is meant to replace.

China has promoted the protocol, along with other homegrown technologies like the 3G standard TD-SCDMA, as part of a vision to produce more of its own technology and have it adopted by international companies.

China Unicom chairman and CEO Chang Xiaobing earlier this year said (http://www.macworld.com/article/146814/2010/03/iphone_wifi_china.html) the company was in talks with Apple about offering a version of the iPhone with Wi-Fi.

The new Apple device, like all mobile phones, still must obtain a network access license from regulators if its maker wants to sell it in China.

Dell is another company that has added WAPI to devices for China (http://www.pcworld.com/businesscenter/article/194002/pictures_of_new_dell_3g_phone_put_on_china_regulator_site.html). Its latest device to support the protocol, a previously unknown TD-SCDMA mobile phone called the Mini 3v, was also cleared last month to use its frequency range, according to the Chinese monitoring center.

Spokeswomen at Apple and Dell did not immediately reply to requests for comment.

Exhibit 11

merics
Mercator Institute
for China Studies

China Monitor

Issue 22 | 21 April 2015
Revised Version 22 April 2015

Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses

Cyber sovereignty, intensified internet censorship, shadow IT economy.

by Hauke Johannes Gierow

MAIN FINDINGS AND CONCLUSIONS

- China is resolutely moving forward with development of its own IT industry. It is also isolating itself from international IT technology. By exercising control over major state-run businesses, the PRC is also maintaining its sovereign position in the IT sector.

- The government supports the international expansion and sales endeavours of Chinese IT companies – the ‘national champions’. This blend of political and economic factors frequently gives rise to security questions among customers from Western countries.

- China is developing parallel standards in the software and hardware sectors. In addition, alternative encryption standards, operating systems and competing app stores are earmarked for enhancing China’s independence in the IT sector. However, inadequate quality regulations are posing a threat to IT security.

- Censorship and restrictions on internet connections place constraints on China as a business location. Concerns about IT espionage and theft of company secrets driving international businesses to transfer personnel or entire departments to other Asian countries.

- Chinese internet users are threatened by a shadow IT economy. Illegal programs are often installed on computers and are not provided with security updates. Hackers can gain access to these unprotected computers and use them as a base for worldwide attacks.

- Instead of insistently calling for fundamental changes in Chinese internet policy, the Federal Government of Germany ought to negotiate specific improvements for German businesses, for example in terms of market access or protection of intellectual property rights.

1 No internet security without independent technology

At the beginning of 2014, an alliance of fifteen private Chinese IT manufacturers was founded in the Beijing district of Zhongguancun (中关村), the Chinese equivalent of Silicon Valley. They stepped up endeavours to develop a Chinese operating system based on Linux that would run on government computers and the computers of security relevant businesses such as banks. **By taking this step, Beijing hopes to gain protection from espionage from the USA and demonstrate the innovative power of the Chinese IT economy.**[1]

In spite of the rampant growth of its IT industry, China is still dependent upon foreign technology at the moment. According to Xinhua, the state news agency, ninety per cent of its microchips and sixty-five per cent of its firewall products originated in other countries in 2012, primarily the US.[2] The government views foreign technology as a potential threat to national security. Covertly installed back doors enable surveillance of computers and networks, for example. Therefore, stringent constraints on the use of foreign IT products are already in place in areas critical to security. At the same time, sealing the domestic market off from external influence is intended to foster the development of industrial and innovation policies in China: the government in Beijing wants to strengthen the competitiveness of domestic IT companies[3] (see issue 20 of MERICS China Monitor).

2 Cyber security: opportunities and costs for the Chinese IT economy

2.1 Targeted promotion by the state

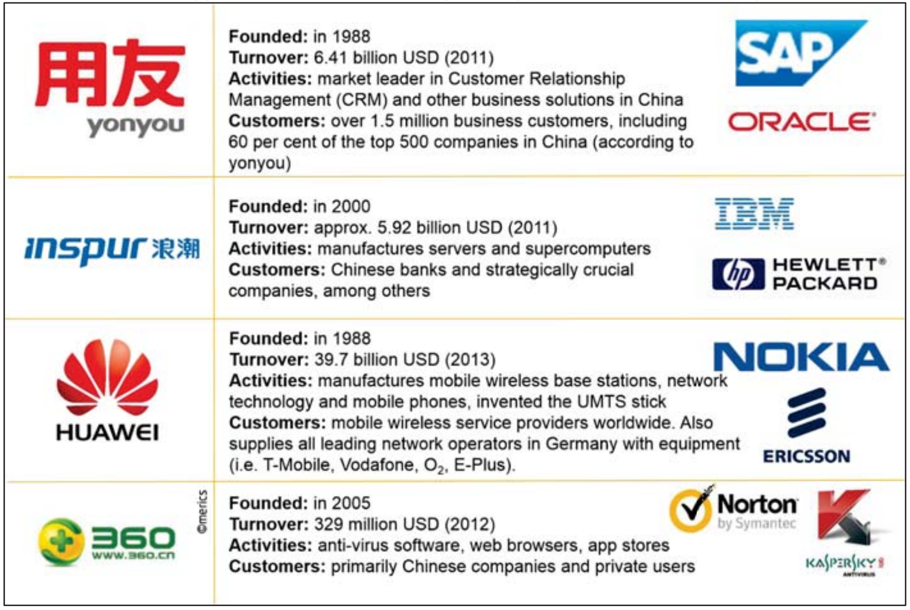
The Chinese government has succeeded in promoting a dynamic IT industry with robust private companies while retaining control over the sector. State-run telecommunications companies (China Telecom, China Unicom and China Mobile) dominate the market with their investments. Decisions they make, usually approved by the government, determine what kind of technologies will be developed, thus defining the framework conditions for the industry and its regulation.[4] In addition, the government promotes its own technological standards through state-run programs, generally in close collaboration with Chinese IT companies such as ZTE, Lenovo and Datang Mobile.

Chinese companies are becoming increasingly successful in the field of IT infrastructure, a fact that is partly due to state support. In addition to Huawei and ZTE, both network equipment suppliers of international repute, new companies are also gaining a foothold in the market now: businesses such as Inspur and Dawning Industries (曙光) are using Chinese technology to develop servers and supercomputers for complex computing tasks, up to now mostly for the domestic market (see Figure 1). **This technology is particularly relevant to secure networks since even small mistakes in the programming code can destroy the basis for secure IT products.**

China will become more independent of foreign IT products in the years to come. However, there is no consensus among experts on whether this independence will enhance network security on the whole. Meeting quality standards, for instance by monitoring the supply chain or having an independent examination of the source code, is a crucial criterion for software security. Many IT companies in China ignore these standards, though.

Encryption technologies are a different problem: This part of the IT infrastructure not only protects hard drives and documents, but it also shields internet connections from unauthorised access. However, the strict import regulations imposed on Chinese companies only allow them to adopt international encryption standards such as RSA, which is used by many governments and corporations, in exceptional cases. Instead, they must rely on Chinese encryption methods, which only provide partial protection. Chinese suppliers have to deposit a type of 'skeleton key' with the National Encryption Leading Group (国家密码管理局) (referred to as the Key Escrow procedure).[5] This procedure protects data from hackers and foreign governments, but the government in Beijing can gain access to it at any time via the skeleton key.

Figure 1: Chinese IT suppliers and their Western competitors (by the author, Hauke Gierow)



用友 yonyou	**Founded:** in 1988 **Turnover:** 6.41 billion USD (2011) **Activities:** market leader in Customer Relationship Management (CRM) and other business solutions in China **Customers:** over 1.5 million business customers, including 60 per cent of the top 500 companies in China (according to yonyou)	SAP ORACLE
inspur 浪潮	**Founded:** in 2000 **Turnover:** approx. 5.92 billion USD (2011) **Activities:** manufactures servers and supercomputers **Customers:** Chinese banks and strategically crucial companies, among others	IBM hp HEWLETT PACKARD
HUAWEI	**Founded:** in 1988 **Turnover:** 39.7 billion USD (2013) **Activities:** manufactures mobile wireless base stations, network technology and mobile phones, invented the UMTS stick **Customers:** mobile wireless service providers worldwide. Also supplies all leading network operators in Germany with equipment (i.e. T-Mobile, Vodafone, O_2, E-Plus).	NOKIA ERICSSON
360 www.360.cn	**Founded:** in 2005 **Turnover:** 329 million USD (2012) **Activities:** anti-virus software, web browsers, app stores **Customers:** primarily Chinese companies and private users	Norton by Symantec KASPERSKY

©merics

2.2 Going out – both an opportunity and challenge for Chinese companies

With their products, Chinese IT firms are stepping up competition with Western companies in developing and emerging countries.

The Chinese Ministry for Industry and Informatisation （中华人民共和国工业和信息化部) has pursued the '*Going Out*' strategy (走出去) ever since 1999. This is used to support successful Chinese companies and make them internationally competitive. It has been expanded to include the IT sector as well. Low-interest loans and the active support of Chinese embassies are the tools with which the government intends to enhance the competitiveness of these national champions on international markets.[6] Huawei, for example, was granted a low-interest loan of ten billion USD by the China Development Bank to finance its international expansion.[7]

But this systematic promotion of the IT sector also presents problems for Chinese companies: technology from the PRC is perceived as a threat to security by other countries, even though there has been no concrete evidence that the government has placed any back doors in routers, mobile phones or other devices to date. Huawei offered to equip the London Underground with mobile wireless technology for the 2012 Olympic Games free of charge, an offer worth more than 500 million CNY (approx. 65 million EUR), but the British side rejected the offer for security reasons.[8]

Both businesses and the Chinese government are now trying to stem the loss of confidence in their products. Huawei, for example, has launched a transparency drive to deal with concerns in Europe. The company has established a research centre in the UK to enable independent security audits of their program code by the British government.[9]

The world’s third-largest mobile phone manufacturer, Xiaomi (小米), is employing a different tactic: to eliminate concerns about back doors in their own cloud services in China, the company is setting up ‘local clouds’ in key markets such as India. Local users can deposit their contacts, calendar entries and other data there instead of in China. This measure is probably intended to build up user confidence in the brand more than anything else, however.

In spite of initial misgivings, Chinese companies are already enjoying great success in some foreign markets. Huawei and Lenovo now rank among the leading manufacturers of IT products for the European and American consumer market, for example. Lenovo actually overtook Hewlett-Packard, the previous market leader in the PC sector, in 2014 by securing a market share of almost seventeen per cent.[10]

Chinese IT companies even keep pace with global leaders in the area of mobile-communications infrastructure. While the Chinese alternative to UMTS, TD-SCMA, is only used in Nicaragua and Zimbabwe outside China, networks with the new Chinese FDD-LTE are part of network infrastructure in Germany and other European countries.

2.3 Alternative ecosystems: their own app stores and operating systems, but with security gaps

Users in China are situated in a unique digital ecosystem. Chinese alternatives have been developed for many applications from the West.

In Germany, users of Android devices download apps or digital content such as films and books primarily through Google’s own app store, *Google Play.* However, *Google Play* is blocked in China, and companies such as Baidu, Tencent or Qihoo 360 offer alternative app stores. Compared to *Google Play,* however, they have severe security drawbacks. A review of 7,000 apps infested with viruses revealed that 95 per cent of them were offered in Chinese app stores.[11] A mobile-phone virus developed by a student infected over 100,000 Android devices in China within only a few hours. The virus spread via the user’s address book and enabled control over almost all of the device’s telephone functions.[12]

The Chinese government also plans to distribute alternative systems on the PC market. For more than five years, it has therefore been pushing the development of its own operating systems hard. From 2015 onwards, fifteen per cent of all computers in every official office are to be converted from Windows to Chinese operating systems. The best-known systems are *NeoKylin OS* and *Red Flag Linux.* Chinese technologies have not reached full maturity yet, however: users complain about compatibility problems, lack of software alternatives and inadequate user-friendliness – a deficit expected to be eliminated by domestic IT companies forming an alliance, as mentioned earlier.

2.4 The high cost of internet censorship

Isolationism and protectionism lead to another problem for Chinese IT companies: the obligation to censor the internet. Not only does censorship affect freedom of speech, but it also impacts the entire economy.

Operating a social network in China is expensive. The State Council Internet Information Office (国家互联网信息办公室) places tight restrictions on information from the internet. To comply with these controls, ISPs are required to employ two to three censors per 50,000 users.[13] For Sina Weibo, with around 300 million users, this means employing 15,000 people for the sole purpose of monitoring the content of the web pages the users invoke – a huge undertaking with considerable financial repercussions. By comparison, the sector's leader, Facebook, employs a total of only 8,500 staff worldwide.[14]

Internet censorship also impairs the development of software and apps. Google and other ISPs grant developers global access to program libraries and web fonts free of charge. This service helps programmers save time and money. Since data in China is blocked by internet censorship, programmers there have to redevelop the data themselves.[15]

3 *Cyber security* – a key location factor for foreign companies

3.1 Censorship and cyber attacks hurt business

Foreign companies in China must comply with ever more stringent regulations in the IT sector, impeding their ability to protect business secrets and hindering international co-operation.

China represents the largest market in the world for Apple; the iPhone is very popular there. In October 2014 it became known that hackers had targeted data transmission to the company's iCloud service. Due to the complexity of the hack, IT experts suspect that the Chinese government was behind the attack or at least knew about it.[16] However, just a few days later, Apple's chief executive, Tim Cook, went to Beijing and held discussions with key decision-makers at party headquarters, Zhongnanhai (中南海). This shows that Beijing has to deal with security reservations on the part of large Western companies in spite of its market power.[17]

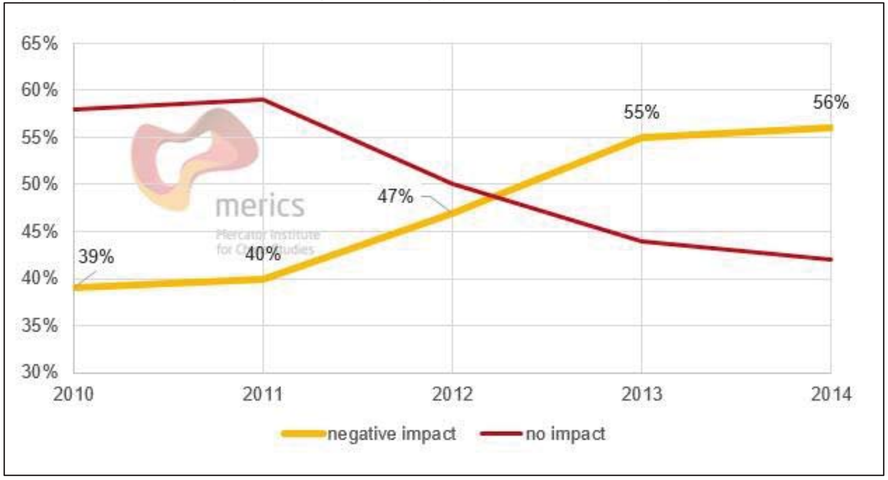
Other companies also feel the impact of cyber attacks and censorship. International collaboration with services such as Gmail, Google Docs or Dropbox is becoming increasingly dysfunctional. The same applies for virtual private networks (VPNs), with which users seek protection for information and business secrets. [18] Routine workflows of global corporations only function to a limited extent in the People's Republic of China. In international companies, for instance, many business applications such as statistics and database programs are not run on local computers, but rather on servers based at corporate headquarters. If connections are slow or VPNs unstable, these applications cannot always be accessed from China. Even simply transferring files to colleagues in other countries can be a trying experience.

More than half the American companies questioned in a recent survey by the American Chamber of Commerce in China indicated that internet censorship is detrimental to their business (see Figure 2).[19] Recently stepped-up blockades of websites and online tools have accelerated this tendency even further. Over eighty per cent of the European companies in China report of negative impact on their business prospects. Thirteen per cent have even postponed investments in R&D due to current events.[20]

The media report that international corporations such as General Motors are already in the process of moving their Asian headquarters to Singapore, Japan or Vietnam. Their reasons for doing so include not only censorship, but also factors such as poor air quality and inadequate protection of intellectual property.[21]

Many companies, including those in the digital sector, have been complaining about industrial espionage for years. Company secrets and construction plans are favourite targets of Chinese hackers.

Figure 2: Internet censorship and competitiveness (by the author, Hauke Gierow)



Question asked: How does censorship of content on the internet impact the ability of your company to conduct routine business in China? Source: AmCham China (2014): 15f.

American cyber-security companies and the FBI blame the Chinese government for supporting and even engaging hackers. Hard evidence of this is scarce, however, as professional hackers are capable of covering their tracks or leaving false trails.

3.2 Parallel technical standards are a challenge to Western companies

Western suppliers on the Chinese market have to conform to parallel Chinese IT standards. The Chinese wireless LAN technology called WAPI

('WLAN Authentication and Privacy Infrastructure') is one example. Even though WPA2 encryption has become the international standard, China has deliberately gone separate ways since 2003. For foreign suppliers of routers and WLAN-compatible devices, this means they have to share their source code with one of eleven licensed Chinese IT companies and contribute to the development of the WAPI standard. Due to insufficient WAPI support, Apple was not allowed to sell the first version of its iPhone in China in 2010 until adjustments were made.[22]

Now, Apple will be the first Western IT company to have its products tested in China for compatibility with Chinese security standards. Lu Wei, head of the State Council Internet Information Office, made an announcement to this effect in January 2015. Thus, the company is presumably sharing confidential information with the government.[23] IT companies such as CISCO, Qualcomm and Microsoft will also have to make concessions if they want to enjoy continued access to the Chinese market in the future.[24]

4 Illegal IT shadow economy

4.1 Piracy poses a security problem

Disputes between Chinese and Western IT companies over their market share and market access are rather secondary to the security of users in China. For them, it is imperative that they are able to shop securely online and that their computers cannot be hacked.

There are major electronics markets in cities such as Shenzhen and Hong Kong. Visitors have a wide selection of software and hardware products to choose from, many of which are manufactured and distributed illegally, however.

Software piracy is clearly harmful to Western manufacturers: according to their own figures, they lose billions in licence fees. Former Microsoft head Steve Ballmer, for instance, once indicated that ninety per cent of the company's products in China were being used illegally.[25] What's more, pirated copies generally do not include any security updates, a fact that is especially problematical in key components such as operating systems. Susceptible devices are not only a security hazard for their users, they also threaten network security worldwide:[26] if security gaps are not closed up, criminals can gain access to users' devices and employ these as 'zombie computers' in botnets. This enables them to steal additional access data from users or attack websites or network infrastructure. Illegally sold operating systems also frequently contain deliberately embedded viruses.

4.2 Hacker networks in China

Criminal hackers are a menace to the well-being and privacy of Chinese internet users. Illegal services are unabashedly offered in public forums, so there is obviously little fear of prosecution.

The ways and means with which illegal services are offered and advertised in China differ fundamentally from those in Western countries. While trade in stolen passwords or credit-card data generally runs via encrypted networks, Chinese hackers co-ordinate their illegal activities in open chat groups in QQ or forums run by Baidu. One reason for this is that Tor[27], an internet anonymizer service, is blocked in China.

A wide variety of often reasonably priced services is offered. Criminals can purchase access to servers with which they can infect users with

merics
Mercator Institute for China Studies

China Monitor

Issue 22 | 21 April 2015

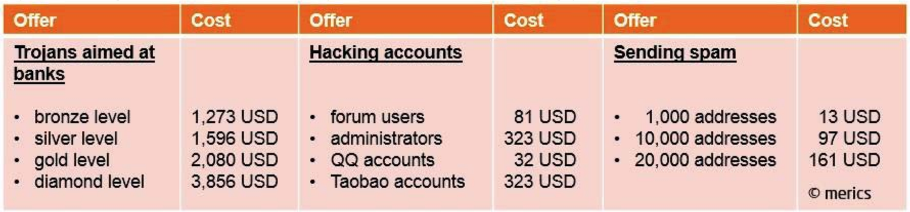
malware or send spam messages. Custom-made Trojan horses or creation of counterfeit sign-in pages for banks and social networks are also available – thus, PCs and smartphones can also be spied on (see Figure 3).

5 German policy against Chinese protectionism

China's steady expansion of its own IT industry and growing isolation from foreign products have been felt keenly by international manufacturers. Germany's cyber policy towards China must be prepared for conflict. In the long run, China will not agree to become integrated into a cyber-security system defined by Western concepts. In fact, Beijing is already working with other newly industrialised countries on parallel standards for internet governance, which has been dominated by the West up to now.

As far as IT services and products for high-tech sectors are concerned – for instance in the area of Industry 4.0 and specialised business software – German companies can rely on their competitiveness in the face of Chinese rivals. The question is, for how much longer? It would therefore be wise for Germany to pursue a policy that has already proved to be effective in other fields.[28] Instead of working towards fundamental change in Chinese cyber security, the Federal Government of Germany should focus on pragmatic goals that are attainable in practice. After all, there are enough urgent topics to be dealt with as it is, such as better protection of intellectual property or secure market access for German companies.

Figure 3: Sample of 'services' offered by criminal hacker networks (by the author, Hauke Gierow)



Offer	Cost	Offer	Cost	Offer	Cost
Trojans aimed at banks		**Hacking accounts**		**Sending spam**	
• bronze level	1,273 USD	• forum users	81 USD	• 1,000 addresses	13 USD
• silver level	1,596 USD	• administrators	323 USD	• 10,000 addresses	97 USD
• gold level	2,080 USD	• QQ accounts	32 USD	• 20,000 addresses	161 USD
• diamond level	3,856 USD	• Taobao accounts	323 USD		
					© merics

Source: Trend Micro (2013).

Your contact for this issue of *China Monitor*:
Hauke Gierow
Hauke.Gierow@merics.de
Editor: Silke Ballweg

Publisher's details:
Mercator Institute for China Studies
Klosterstr. 64
D-10179 Berlin
phone: +49 30 3440 999-0
e-mail: info@merics.de
www.merics.org

[1] Zhang, Yu (2014). 'Homegrown developers look to unseat Microsoft's dominant OS', http://www.globaltimes.cn/content/887716.shtml. Accessed on 24 October 2014.

[2] Zhangwei 张卫 (2012). '信息安全的机遇与挑战' (Opportunities and Challenges of Information Security). http://news.sohu.com/20120416/n340660958.shtml. Accessed on 15 September 2014.

[3] Zhonghua renmin gongheguo guowuyuan 中华人民共和国国务院 (2012). '国务院出台意见推进信息化发展切实保障信息安全' (The State Council publishes a document on promoting the development of informatisation and for the protection of cyber security). http://politics.gmw.cn/2012-07/17/content_4571519.htm. Accessed on 14 August 2014.

[4] Ernst, Dieter and Naughton, Barry (2008). 'China's emerging industrial economy: insight from the IT industry', in: McNally, Christopher A. (ed.) (2008). *China's Emergent Political Economy – Capitalism in the dragon's lair*, 39–59. London and New York: Routledge.

[5] Cloutier, Christopher T. and Cohen, Jane Y. (2011). 'Casting a wide net: China's encryption restrictions', http://www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf. Accessed on 15 August 2014.

[6] Wang, Yukai 汪玉凯 (2014). '中央网络安全与信息化领导小组的由来及其影响' (The origins and impact of the Central Cyber Security and Informatisation Leading Group). http://theory.people.com.cn/2014/0303/c40531-24510897.html. Accessed on 22 October 2014.

[7] Nolan, Peter (2014). *Chinese Firms, Global Firms: Industrial Policy in the Era of Globalisation*. New York: Routledge.

[8] Fauna (2011). 'Huawei's London Underground Bid Blocked, Chinese Reactions', http://www.chinasmack.com/2011/stories/huaweis-london-underground-bid-blocked-chinese-reactions.html. Accessed on 30 November 2014.

[9] Kan, Michael (2013). 'UK to probe Huawei's cybersecurity evaluation center', http://www.pcworld.com/article/2044722/uk-to-probe-huaweis-cybersecurity-evaluation-center.html. Accessed on 22 October 2014.

[10] Gartner (2014). 'Gartner Says Worldwide PC Shipments Declined 6.9 Percent in Fourth Quarter of 2013', http://www.gartner.com/newsroom/id/2647517. Accessed on 22 September 2014.

[11] Eddy, Max (2013). 'Nearly 7,000 Malicious Android Apps Infest China's Appstores', http://securitywatch.pcmag.com/mobile-security/315218-nearly-7-000-malicious-android-apps-infest-china-s-appstores. Accessed on 22 September 2014.

[12] Muncaster, Phil (2014). 'Chinese Heart App Virus Slams 100,000 Android Phones', http://www.infosecurity-magazine.com/news/chinese-virus-100000-android-phones/. Accessed on 22 September 2014.

[13] King, Gary, Pan, Jennifer and Roberts, Margaret E. (2014). 'Reverse-engineering censorship in China: Randomized experimentation and participant observation', *Science* 345 (6199): 1–10.

[14] Facebook Newsroom (2014). Company Info. http://newsroom.fb.com/company-info/. Accessed on 30 November 2014.

[15] Bradsher, Keith and Mozur, Paul (2014). 'China Clamps Down on Web, Pinching Companies Like Google', http://www.nytimes.com/2014/09/22/business/international/china-clamps-down-on-web-pinching-companies-like-google.html?_r=0. Accessed on 25 September 2014.

[16] Franceschi-Bicchierai, Lorenzo (2014). 'Apple Addresses iCloud Attacks While China Denies Hacking Allegations', http://mashable.com/2014/10/21/apple-icloud-attacks-china/. Accessed on 22 October 2014.

[17] Lovejoy, Ben (2014). 'Tim Cook meets with Chinese vice premier in Beijing following iCloud phishing attack', http://www.techgreatest.com/apple-news/tim-cook-meets-with-chinese-vice-premier-in-beijing-following-icloud-phishing-attack/. Accessed on 3 December 2014.

[18] Arthur, Charles (2011). 'China cracks down on VPN use', http://www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use. Accessed on 3 December 2014.

[19] American Chamber of Commerce in China (2013). 'Business Climate Survey 2013', http://web.resource.amchamchina.org/cmsfile/2013/03/29/0640e5a7e0c8f86ff4a380150357bbef.pdf. Accessed on 24 September 2014.

[20] The European Chamber of Commerce in China (2015). 'Internet Restrictions Increasingly Harmful to Business, say European Companies in China', http://www.europeanchamber.com.cn/en/press-releases/2235/internet_restrctions_increasingly_harmful_to_business_says_european_companies_in_china. Accessed on 17 February 2015.

[21] Bradsher, Keith (2014). 'Looking Beyond China, Some Companies Shift Personnel', http://www.nytimes.com/2014/09/10/business/international/looking-beyond-china-some-companies-shift-personnel.html?_r=0. Accessed on 30 November 2014.

[22] Ricker, Thomas (2010). 'Chinese iPhone approved with WAPI WiFi', http://www.engadget.com/2010/05/04/chinese-iphone-approved-with-wapi-wifi/. Accessed on 30 November 2014.

[23] Shouji zhongguo wang 手机中国网 (2015). '苹果成全球首个接受中方网络安全审查的公司' (Apple will be the world's first company to have network security tested by the Chinese), http://t.m.china.com.cn/convert/c_uPId9W.html. Accessed on 22 January 2015.

[24] Mozur, Paul (2015). 'New Rules in China Upset Western Tech Companies', http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?ref=business&_r=0. Accessed on 2 February 2015.

[25] Brodkin, Jon (2011). 'Ballmer to Hu: 90% of Microsoft customers in China using pirated software', http://www.networkworld.com/article/2199038/software/ballmer-to-hu--90--of-microsoft-customers-in-china-using-pirated-software.html. Accessed on 30 November 2014.

[26] Gantz, John F. et al. (2013). 'The Dangerous World of Counterfeit and Pirated Software', white paper no. 239751.

http://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf. Accessed on 22 October 2014.

[27] The Onion Routing (Tor). One way to circumvent Internet censorship.

[28] Heilmann, Sebastian (2014). 'Lob der Nischenpolitik – Deutschland spielt in Europas China-Politik heute die Rolle des Impulsgebers' (In praise of niche politics: Germany plays the part of the initiator in China's current policy'), *Internationale Politik*, September/October, 34–43.

Exhibit 12

BUSINESS / Technology

While it defies U.S. government, Apple abides by China's orders — and reaps big rewards

China surpassed the U.S. last year as the No. 1 buyer of iPhones and could one day be the largest market for Apple Pay. Above, an Apple store in Beijing. (Wu Hong / EPA)

By **David Pierson · Contact Reporter**

FEBRUARY 26, 2016, 3:00 AM

Apple Inc. has come out swinging in its pitched battle with the government on its home turf.

But when it comes to its second-largest market, China, the Cupertino, Calif., company has been far more accommodating.

Since the iPhone was officially introduced in China seven years ago, Apple has overcome a national security backlash there and has censored apps that wouldn't pass muster with Chinese authorities. It has moved local user data onto servers operated by the state-owned China Telecom and submits to security audits by Chinese authorities.

The approach contrasts with Apple's defiant stance against the FBI, which is heaping pressure on the company to decrypt an iPhone that belonged to San Bernardino shooter Syed Rizwan Farook.

> “
>
> **I can't imagine the Chinese would tolerate end-to-end encryption or a refusal to cooperate with their police, particularly in a terrorism case.**
>
> — James Lewis, senior fellow, Center for Strategic and International Studies

The years-long strategy in China is paying off at a crucial time. While sales of Apple products have flatlined or declined in the U.S., Europe and Japan, business in the company's greater China region continues to soar — to a record $59 billion last year. The Asian giant surpassed the U.S. last year as the No. 1 buyer of iPhones and could one day be the largest market for Apple Pay, the mobile payment platform that was rolled out for Chinese consumers last week.

But there's no guarantee the good times will continue rolling for Apple. Beijing is increasingly tightening the screws on foreign technology companies, having introduced strict laws aimed at policing the Internet and digital hardware.

The environment will get even tougher, Apple says, if the FBI prevails in seeking a so-called backdoor to Farook's phone. That could set a precedent for China's authoritarian leaders to demand the same in a country where Apple has never publicly defied orders.

"What's driving this is Apple's desire to persuade the global market, and particularly the China market, that the FBI can't just stroll in and ask for data," said James Lewis, senior fellow at the Center for Strategic and International Studies in Washington. "I can't imagine the Chinese would tolerate end-to-end encryption or a refusal to cooperate with their police, particularly in a terrorism case."

The last time Apple was in the crosshairs of Chinese negative opinion was after the Edward Snowden National Security Agency leak in late 2013.

Chinese state-run media began raising national security questions about the iPhone's location-tracking feature. Communist party cadres and other officials were also urged to ditch their Apple devices.

The controversy underscored how quickly nationalistic sentiment in China can turn on a foreign brand.

Amid the furor, Apple announced it was shifting local user data onto China-based servers.

The move was seen by some analysts as a concession to calm fears that Apple's infrastructure was compromised by U.S. intelligence. It came four years after Google pulled its search engine out of China in an unprecedented stand against the Chinese government over censorship.

Apple, one of only a handful of U.S. tech giants that have flourished in China, said the move was necessary to improve services for its growing Chinese user base. It added that all data on the servers were encrypted and inaccessible to China Telecom.

Even so, some security experts say the servers could be vulnerable.

"Whatever data is on Chinese servers is susceptible to confiscation or even cryptanalysis," a sort of code cracking, said Jonathan Zdziarski, a leading expert in iPhone security.

The same could be said about access to data in servers in the U.S., Zdziarski said, the only difference being you need a subpoena.

But it's not just the servers that pose a risk. Apple's source codes could be stolen from one of its Chinese factories or during government security audits.

"Most of the hardware tools that have hacked iPhones in the past all came out of China, and that's probably for a reason," Zdziarski said. "It'd be foolish to think that Apple could form a safe and healthy relationship with the Chinese government that didn't put the U.S. at some level of higher risk."

In the end, moving users to China Telecom's servers was followed by a rehabilitation of Apple's image in China that continues today.

See more of our top stories on Facebook >>

On Monday, the state-run Economic Daily gave Apple Pay its stamp of approval, saying it complied with national security standards — echoing endorsements the iPhone 6 received more than a year earlier.

In January 2015, the government mouthpiece, the People's Daily, tweeted a picture of Apple Chief Executive Tim Cook shaking hands with Lu Wei, China's top cyberspace official.

"Apple has agreed to China's security checks, 1st foreign firm to agree to rules of Cyberspace Admin of China," the tweet said.

Apple said this was nothing special; it accedes to security checks in all countries it operates in. And all companies that want to do business with China are required to submit to such checks.

What's different, however, is how stringent the checks could be in the near future.

Despite criticism from foreign governments, including the White House, China is introducing security laws that are so vaguely worded some fear it will require technology companies to provide source codes and backdoors for market access. Regulators there have already demanded more foreign companies store data locally like Apple did with China Telecom.

How the new rules fare could depend on the outcome of Apple's case with the FBI, experts say.

"The problem is, depending on what happens with Apple in the U.S., the window for foreign companies to maneuver over encryption and other security requirements in China could shrink," said Samm Sacks, an analyst for Eurasia Group.

She said the ambiguity of China's security laws are designed to promote self-censorship.

Apple in the past has pulled apps from its China app store that mentioned the Dalai Lama and ethnic Uighur activist Rebiya Kadeer — both considered enemies of the state. And late last year, it disabled its news app in China.

"Virtually every foreign tech company doing business in China is going to have to make some concessions to the government, just as the price of entry," said Charlie Custer, a writer and expert on tech in China.

"I'd love to hold all global corporations to Google's moral standard, but it's probably not realistic to expect that, especially from a company like Apple whose most important market is probably China."

david.pierson@latimes.com

Exhibit 13

Legal Process Guidelines

U.S. Law Enforcement

These Guidelines are provided for use by law enforcement or other government entities in the U.S. when seeking information from Apple Inc. (“Apple”) about users of Apple’s products and services, or from Apple devices. Apple will update these Guidelines as necessary. This version was released on September 29, 2015.

All other requests for information regarding Apple users, including user questions about disclosure of information, should be directed to http://www.apple.com/privacy/contact/. These Guidelines do not apply to requests that law enforcement agencies make outside the U.S. to Apple’s relevant local subsidiaries.

For government information requests, we comply with the laws pertaining to global entities that control our data and we provide details as legally required. For content requests from law enforcement agencies outside the U.S., with the exception of emergency circumstances (defined in the Electronic Communications Privacy Act 1986, as amended), Apple will only provide content in response to a search warrant issued pursuant to the Mutual Legal Assistance Treaty process or through other cooperative efforts with the United States Department of Justice.

INDEX

I. General Information

Apple designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store. User information is held by Apple in accordance with Apple's privacy policy and the applicable terms of service/terms and conditions for the particular service offering. Apple is committed to maintaining the privacy of the users of Apple products and services ("Apple users"). Accordingly, information about Apple users will not be released without proper legal process.

The information contained within these Guidelines is devised to provide information to law enforcement agencies regarding the legal process that Apple requires in order to disclose electronic information to law enforcement and government agencies. These Guidelines are not intended to provide legal advice. The frequently asked questions ("FAQ") section of these Guidelines is intended to provide answers to some of the more common questions that Apple receives. Neither these Guidelines nor the FAQ will cover every conceivable circumstance that may arise. Accordingly, please contact subpoenas@apple.com with any further questions. This email address is intended solely for use by law enforcement and government agents. If you choose to send an email to this address, it must be from a valid government email address. Nothing within these Guidelines is meant to create any enforceable rights against Apple and Apple's policies may be updated or changed in the future without further notice to law enforcement.

The majority of subpoenas, search warrants, and court orders that Apple receives seek information regarding a particular Apple device or customer and the specific service(s) that Apple may provide to that customer. Apple can provide Apple device or customer information in so far as Apple still possesses the requested information pursuant to its data retention policies. Apple retains data as outlined in certain "Information Available" sections below. All other data is retained for the period necessary to fulfill the purposes outlined in our privacy policy. Law enforcement should be as narrow and specific as possible when fashioning their legal process to avoid misinterpretation and/or objections in response to an overly broad request. Law enforcement is required to obtain a search warrant that is issued upon a probable cause showing for search warrants requesting user content.

II. Service of Process Guidelines

A. Service of Law Enforcement Subpoenas, Search Warrants, and Court Orders

Apple will accept service of subpoenas, search warrants, and court orders for information by email from law enforcement agencies, provided these are transmitted from the official email address of the law enforcement agency concerned. Law enforcement officers submitting a legal request to Apple should transmit it directly from their official law enforcement email address to the mailbox subpoenas@apple.com.

Please serve process in PDF format via an official law enforcement/government email address directly and exclusively to:

subpoenas@apple.com

Apple Inc.
Attention: Privacy and Law Enforcement Compliance
1 Infinite Loop, Cupertino, CA 95014

The above email address is intended solely for use by law enforcement and government agents. When law enforcement has served legal process on Apple by email to subpoenas@apple.com, in order to prevent disproportionate effort, there is no need to serve duplicate hardcopy process on Apple by mail.

We require law enforcement to include the following information with the legal request so the request can be verified:

Law Enforcement Agency
Law Enforcement Agent Name and Badge/ID number
Agency issued email address
Law Enforcement Phone number (with extension if applicable)
Verifiable physical return address
Law Enforcement Fax number

Note: All matters that are not law enforcement related must be either personally served at Apple's headquarters in Cupertino, California or served through CT Corporation (Apple's registered agent for service of process). For any inquiries related to law enforcement legal process, please contact: subpoenas@apple.com. If you are inquiring regarding the status of a specific subpoena, search warrant, or court order, please do not contact Apple until at least 10 business days after service of your request unless the matter involves imminent harm or threat to life.

B. Witness Testimony Subpoenas

Apple will not waive service requirements for subpoenas seeking witness testimony nor accept service via electronic means. All subpoenas seeking witness testimony must either be personally served on Apple or served through Apple's registered agent for service of process. Apple will resist subpoenas for witness testimony that are served with fewer than 14 days advance notice.

C. Preservation Requests

Requests to preserve information pursuant to 18 U.S.C. § 2703(f) should be directed to Apple's Privacy and Law Enforcement Compliance Group by email to subpoenas@apple.com. Please submit preservation requests on law enforcement letterhead with the agent and agency identified within the letter and include a valid government email address and phone number in the letter so the request can be verified.

Preservation requests must include the relevant Apple ID/account email address, or full name **and** phone number, and/or full name **and** physical address of the subject Apple account. When a preservation request has been received, Apple will preserve a one-time data pull of the requested existing user data available at the time of the request for 90 days. After this 90 day period, the preservation will be automatically removed from the storage server. However, this period can be extended one additional 90-day period upon a renewed request. More than two preservations for the same account will be treated as requests for an extension of the originally preserved materials, but Apple will not preserve new material in response to such requests.

D. Emergency Disclosure

The Electronic Communications Privacy Act ("ECPA") covers the authorized disclosure of content by Apple. An exception to the requirement that law enforcement obtain a search warrant for customer content is provided by ECPA in situations in which the case involves an emergency. Under 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4) Apple is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay.

In order to request that Apple voluntarily disclose information on an emergency basis, please fill out the Emergency Law Enforcement Information Request form available at Appendix A and send a copy of the completed form by email to the mailbox: exigent@apple.com and include "Emergency Law Enforcement Information Request" in the subject line.

In the event that Apple produces customer data in response to an Emergency Law Enforcement Information Request, a supervisor for the law enforcement agent who submitted the Emergency Law Enforcement Information Request will be contacted and will be asked to confirm to Apple that the emergency law enforcement information request was legitimate. Apple requires that the law enforcement agent who submits the Emergency Law Enforcement Information Request provide the supervisor's contact information upon submission of the request.

If you need to contact Apple after hours (before 8:00 am or after 5:00 pm Pacific time) for an emergency inquiry, please contact Apple's Global Security Operations Center (GSOC) at (408) 974-2095.

E. Account Deletion Requests

In the event that law enforcement is requesting that Apple delete a customer's Apple ID, law enforcement is required to provide Apple with a court order or warrant specifying the account that is to be deleted and the basis for the request.

F. User Notice

Apple will notify its customers when their personal information is being sought in response to legal process except where providing notice is prohibited by the legal process itself, by a court order Apple receives (e.g., an order under 18 U.S.C. §2705(b)), or by applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.

Apple will provide delayed notice for emergency disclosure requests except where notice is prohibited by court order or applicable law or where Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment. Apple will provide delayed notice for requests after expiration of the non-disclosure period specified in a court order unless Apple, in its sole discretion, believes that providing notice could create a risk of injury or death to an identifiable individual or group of individuals or in situations where the case relates to child endangerment.

III. Information Available From Apple

A. Device Registration

Basic registration or customer information, including, name, address, email address, and telephone number is provided to Apple by customers when registering an Apple device prior to iOS 8 and OS Yosemite 10.10. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running OS Yosemite 10.10 and later versions is received when a customer associates a device to an iCloud Apple ID. This information may not be accurate or reflect the device's owner. Registration information can be obtained with a subpoena or greater legal process.

Please note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. Requests for serial numbers with either the letter "O" or "I" will yield no results.

B. Customer Service Records

Contacts that customers have had with Apple customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available. This information can be obtained with a subpoena or greater legal process.

C. iTunes

iTunes is a free software application which customers use to organize and play digital music and video on their computers. It's also a store that provides content for customers to download for their computers and iOS devices. When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections may also be available. iTunes subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. iTunes purchase/download transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific content purchased or downloaded.

D. Apple Retail Store Transactions

Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple Retail Store. A subpoena or greater legal process is required to obtain information regarding the type of card associated with a particular purchase, name of the purchaser, email address, date/time of the transaction, amount of the transaction, and store location. When providing legal process requesting Point of Sale records, include the complete credit/debit card number used and any additional information such as date and time of transaction, amount, and items purchased. Additionally, law enforcement may provide Apple with the receipt number associated with the purchase(s) in order to obtain duplicate copies of receipts, in response to a subpoena or greater legal process.

E. Apple Online Store Purchases

Apple maintains information regarding online purchases including name, shipping address, telephone number, email address, product purchased, purchase amount, and IP address of the purchase. A subpoena or greater legal process is required in order to obtain this information. When requesting information pertaining to online orders (excluding iTunes purchases), a complete credit/debit card number, an order number, reference number, or serial number of the item purchased. A customer name in combination with these parameters may also be provided, but customer name alone is insufficient to obtain information.

F. iTunes Gift Cards

iTunes gift cards have a sixteen-digit alphanumeric redemption code which is located under the “scratch-off” gray area on the back of the card, and a nineteen-digit code at the bottom of the card. Based on these codes, Apple can determine whether the card has been activated[1] or redeemed as well as whether any purchases have been made on the account associated with the card. When iTunes gift cards are activated, Apple records the name of the store, location, date, and time. When iTunes gift cards are redeemed through purchases made on the iTunes Store, the gift card will be linked to a user account. iTunes gift cards purchased through the Apple Online Store can be located in Apple systems by their Apple Online Store order numbers (note: this only applies to iTunes gift cards purchased through Apple as opposed to third-party retailers). Information regarding the customer who redeemed the cards will require a subpoena, and transactional information about iTunes purchases will require a court order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide specific iTunes content purchased.

Apple is unable to deactivate iTunes gift cards in response to legal process from a law enforcement/ government agency.

G. iCloud

iCloud is Apple’s cloud service that allows users to access their music, photos, documents, and more from all their devices. iCloud also enables subscribers to back up their iOS devices to iCloud. With the iCloud service, subscribers can set up an iCloud.com email account. iCloud email domains can be

[1] Activated means that the card was purchased at a retail point-of-sale but not that it was used or redeemed (i.e., used to increase the store credit balance on an iTunes account or used to purchase content in the iTunes Store).

@icloud.com, @me.com[2] and @mac.com. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers.

iCloud is a subscriber based service. Requests for iCloud data must include the relevant Apple ID/account email address. If Apple ID/account email address are unknown, Apple requires subscriber information in the form of full name **and** phone number, and/or full name **and** physical address to identify the subject Apple account.

The following information may be available from iCloud:

i. Subscriber Information

When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. Connection logs are retained up to 30 days.

ii. Mail Logs

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant. iCloud mail logs are retained up to 60 days.

iii. Email Content

iCloud only stores the email a subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. Apple is unable to provide deleted content. Available email content may be provided in response to a search warrant issued upon a showing of probable cause.

iv. Other iCloud Content. Photo Stream, Docs, Contacts, Calendars, Bookmarks, iOS Device Backups

iCloud only stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud content may be provided in response to a search warrant issued upon a showing of probable cause.

[2] iCloud has replaced the MobileMe service. Accordingly, Apple does not have any separate content associated with former MobileMe accounts. If the content is not in iCloud, it is no longer being stored.

H. Find My iPhone

Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device. More information about this service can be found at http://www.apple.com/icloud/find-my-iphone.html. Location information for a device located through the Find My iPhone feature is user facing and Apple does not have records of maps or email alerts provided through the service. Find My iPhone connection logs may be available and can be obtained with a subpoena or greater legal process. Find My iPhone connection logs are available for a period of approximately 30 days. Find My iPhone transactional activity for requests to remotely lock or erase a device may be available with an order under 18 U.S.C. § 2703(d) or a court order with the equivalent legal standard or a search warrant.

Apple cannot activate this feature on users' devices upon a request from law enforcement. The Find My iPhone feature must have been previously enabled by the user for that specific device. Apple does not have GPS information for a specific device or user.

I. Extracting Data from Passcode Locked iOS Devices

For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 through iOS 7. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party app data.

The data extraction process can only be performed at Apple's Cupertino, California headquarters for devices that are in good working order. For Apple to assist in this process, the language outlined below must be included in a search warrant, and the search warrant must include the serial or IMEI number of the device. For more information on locating the IMEI and serial number of an iOS device, refer to http://support.apple.com/kb/ht4061.

Please make sure that the name of the judge on the search warrant is printed clearly and legibly in order for the paperwork to be completed.

Once law enforcement has obtained a search warrant containing this language, it may be served on Apple by email to subpoenas@apple.com. The iOS device can be provided to Apple for data extraction either through an in person appointment or through shipment. If law enforcement chooses to ship the device, the device should not be shipped unless and until the officer receives an email from Apple requesting shipment.

For an in-person data extraction process, Apple requires that the law enforcement agent bring a FireWire hard drive with a storage capacity of at least two times the memory capacity for the iOS device. Alternatively, if law enforcement chooses to ship the device, law enforcement should provide Apple with an external hard drive or USB "thumb" drive with a storage capacity of at least two times the memory capacity for the iOS device. Please do not send the device unless and until you receive an email requesting its shipment.

After the data extraction process has been completed, a copy of the user generated content on the device will be provided. Apple does not maintain copies of any user data extracted during the process; accordingly all evidence preservation remains the responsibility of the law enforcement agency.

Required Search Warrant Language:

> "It is hereby ordered that Apple Inc. assist [LAW ENFORCEMENT AGENCY] in its search of one Apple iOS device, Model #______________, on the ________ network with access number (phone number) __________, serial[3] or IMEI[4] number ____________, and FCC ID#_______________ (the "Device"), by providing reasonable technical assistance in the instance where the Device is in reasonable working order and has been locked via passcode protection. Such reasonable technical assistance consists of, to the extent possible, extracting data from the Device, copying the data from the Device onto an external hard drive or other storage medium, and returning the aforementioned storage medium to law enforcement. Law Enforcement may then perform a search of the device data on the supplied storage medium.
>
> It is further ordered that, to the extent that data on the Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data.
>
> Although Apple shall make reasonable efforts to maintain the integrity of data on the Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents."

J. Other Available Device Information

MAC Address: A Media Access Control address (MAC address), is a unique identifier assigned to network interfaces for communications on the physical network segment. Any Apple product with network interfaces will have one or more MAC addresses, such as Bluetooth, Ethernet, Wi-Fi, or

[3] Note, Apple device serial numbers do not contain the letters "O" or "I," rather Apple utilizes the numbers 0 (zero) and 1 (one) in serial numbers. iOS extractions for serial numbers with either the letter "O" or "I" can not be performed.

[4] The IMEI number is engraved on the back of cellular iPads, the original iPhone, iPhone 5, 5c, 5s, 6, and 6 Plus. For more information, see http://support.apple.com/kb/ht4061. Note that for models with IMEI numbers engraved on the SIM tray, the SIM tray in the device may not be the matching original that came with the device.

FireWire. By providing Apple with a serial number (or in the case of an iOS device, IMEI, MEID, or UDID), this information may be obtained with a subpoena or greater legal process.

UDID: The unique device identifier (UDID) is a sequence of 40 letters and numbers that is specific to a particular iOS device. It will look similar to following: 2j6f0ec908d137be2e1730235f5664094b831186.

If law enforcement is in possession of the device, the device may be connected to iTunes in order to obtain the UDID. Under the iTunes summary tab, the UDID can be revealed by clicking on the serial number.

K. Requests for Apple Retail Store Surveillance Videos

Video surveillance records may vary by store location. Video surveillance records are typically maintained at an Apple store for approximately thirty days. After thirty days, video surveillance may no longer be available. A request for video surveillance can be made at any local Apple retail store. Law enforcement should provide specific date, time, and related transaction information regarding the video requested.

L. Game Center

Game Center is Apple's social gaming network. Information regarding Game Center connections for a user or a device may be available. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Game Center transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard. A search warrant issued upon a showing of probable cause is required for Apple to provide the specific game(s) played.

M. iOS Device Activation

When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available. This information can be obtained with a subpoena or greater legal process.

N. Sign-on Logs

Sign-on activity for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Sign-on transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

O. My Apple ID and iForgot Logs

My Apple ID and iForgot logs for a user may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions. Connection logs with IP addresses can be obtained with a subpoena or greater legal process. Transactional records can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

P. FaceTime

FaceTime communications are end-to-end encrypted and Apple has no way to decrypt FaceTime data when it is in transit between devices. Apple cannot intercept FaceTime communications. Apple has FaceTime call invitation logs when a FaceTime call invitation is initiated. These logs do not indicate that any communication between users actually took place. Apple has no information as to whether the FaceTime call was successfully established or duration of a FaceTime call. FaceTime call invitation logs are retained up to 30 days. FaceTime call invitation logs can be obtained with an order under 18 U.S.C. §2703(d) or court order meeting the equivalent legal standard or search warrant.

IV. Frequently Asked Questions

Can I email Apple with questions regarding my legal process?

Yes, questions or inquiries regarding government legal process can be emailed to subpoenas@apple.com.

I need to personally serve Apple, where should I go?

All personal service can be made at Apple's Cupertino, California headquarters located at the following address:

Apple Inc.
1 Infinite Loop
Cupertino, CA 95014-2084

Can I serve a deposition subpoena directly on an Apple retail store?

No, all subpoenas for testimony, including subpoenas for deposition or trial testimony, need to be personally served on Apple.

I requested information in the body of my email, why was it not provided?

Requests for information not included within the body of the signed subpoena, search warrant, or court order will be disregarded; all information requested must be in the actual executed legal process document.

Can Apple provide me with the passcode of an iOS device that is currently locked?

No, Apple does not have access to a user's passcode but, depending on the version of iOS that the device is running, may be able to extract some data from a passcode locked iOS device running iOS 4 through iOS 7 with a valid search warrant as described in the Guidelines.

Does a device have to be registered with Apple in order to function?

No, a device does not have to be registered with Apple in order for it to function or be used.

Can you help me return a stolen or lost device to the rightful owner?

In cases where law enforcement has recovered a lost or stolen device and wants to return it to the "original owner," contact Apple Customer Care (ACC) via email at law_enforcement_esc@apple.com. Please include the device's serial number in your email and any additional pertinent information. If registration information is available, ACC will contact the owner and instruct him or her to contact law enforcement to recover the device. A subpoena is not required in most cases. However, if there is conflicting information located within our databases you may be instructed to submit a subpoena.

How will the information requested be delivered?

Responsive production of records and information will be sent in an encrypted electronic container via email or, in some instances, via FedEx delivery. If no responsive information is available, a letter indicating this will be sent via email or, in some cases, via U.S. mail.

I am looking into whether a user's email reach the requirements for interstate commerce. Where are the iCloud email servers located?

Apple's U.S. email servers are located in California, Nevada, North Carolina, and Oregon.

Does Apple store GPS information that can be produced under proper legal process?

No, Apple does not track geolocation of devices.

What should be done with the produced files and records when law enforcement has concluded the investigation/criminal case?

Apple requires that any information and data provided to law enforcement containing personally identifiable information (including any copies made) must be destroyed after the related investigation, criminal case, and all appeals have been fully exhausted.

Do you notify users of criminal legal process?

Yes, Apple's notice policy applies to account requests from law enforcement. Apple will notify customers and account holders unless there is a non-disclosure order or applicable law prohibiting notice, or we believe in our sole discretion that such notice may pose immediate risk of serious injury or death to a member of the public, the case relates to a child endangerment matter, or where notice is not applicable to the underlying facts of the case.

Can Apple intercept users' communications pursuant to a Wiretap Order?

Apple can intercept users' email communications, upon receipt of a valid Wiretap Order. Apple cannot intercept users' iMessage or FaceTime communications as these communications are end-to-end encrypted.

V. Appendix A

As per section II (D) above, to request that Apple voluntarily disclose information on an emergency basis, please fill out the Emergency Law Enforcement Information Request form and submit it via email to exigent@apple.com with "Emergency Law Enforcement Information Request" included in the email subject.

The EMERGENCY Law Enforcement Information Request form is available as an editable PDF at: http://www.apple.com/legal/privacy/le-emergencyrequest.pdf

Exhibit 14

Answers to your questions about Apple and security

Why is Apple objecting to the government's order?

The government asked a court to order Apple to create a unique version of iOS that would bypass security protections on the iPhone Lock screen. It would also add a completely new capability so that passcode tries could be entered electronically.

This has two important and dangerous implications:

First, the government would have us write an entirely new operating system for their use. They are asking Apple to remove security features and add a new ability to the operating system to attack iPhone encryption, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by "brute force," trying thousands or millions of combinations with the speed of a modern computer.

We built strong security into the iPhone because people carry so much personal information on our phones today, and there are new data breaches every week affecting individuals, companies and governments. The passcode lock and requirement for manual entry of the passcode are at the heart of the safeguards we have built in to iOS. It would be wrong to intentionally weaken our products with a government-ordered backdoor. If we lose control of our data, we put both our privacy and our safety at risk.

Second, the order would set a legal precedent that would expand the powers of the government and we simply don't know where that would lead us. Should the government be allowed to order us to create other capabilities for surveillance purposes, such as recording conversations or location tracking? This would set a very dangerous precedent.

Is it technically possible to do what the government has ordered?

Yes, it is certainly possible to create an entirely new operating system to undermine our security features as the government wants. But it's something we believe is too dangerous to do. The only way to guarantee that such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it.

Could Apple build this operating system just once, for this iPhone, and never use it again?

The digital world is very different from the physical world. In the physical world you can destroy something and it's gone. But in the digital world, the technique, once created, could be used over and over again, on any number of devices.

Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the FBI wins this case. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks. Of course, Apple would do our best to protect that key, but in a world where all of our data is under constant threat, it would be relentlessly attacked by hackers and cybercriminals. As recent attacks on the IRS systems and countless other data breaches have shown, no one is immune to cyberattacks.

Again, we strongly believe the only way to guarantee that such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it.

Has Apple unlocked iPhones for law enforcement in the past?

No.

We regularly receive law enforcement requests for information about our customers and their Apple devices. In fact, we have a dedicated team that responds to these requests 24/7. We also provide guidelines on our website for law enforcement agencies so they know exactly what we are able to access and what legal authority we need to see before we can help them.

For devices running the iPhone operating systems prior to iOS 8 and under a lawful court order, we have extracted data from an iPhone.

We've built progressively stronger protections into our products with each new software release, including passcode-based data encryption, because cyberattacks have only become more frequent and more sophisticated. As a result of these stronger protections that require data encryption, we are no longer able to use the data extraction process on an iPhone running iOS 8 or later.

Hackers and cybercriminals are always looking for new ways to defeat our security, which is why we keep making it stronger.

The government says your objection appears to be based on concern for your business model and marketing strategy. Is that true?

Absolutely not. Nothing could be further from the truth. This is and always has been about our customers. We feel strongly that if we were to do what the government has asked of us — to create a backdoor to our products — not only is it unlawful, but it puts the vast majority of good and law abiding citizens, who rely on iPhone to protect their most personal and important data, at risk.

Is there any other way you can help the FBI?

We have done everything that's both within our power and within the law to help in this case. As we've said, we have no sympathy for terrorists.

We provided all the information about the phone that we possessed. We also proactively offered advice on obtaining additional information. Even since the government's order was issued, we are providing further suggestions after learning new information from the Justice Department's filings.

One of the strongest suggestions we offered was that they pair the phone to a previously joined network, which would allow them to back up the phone and get the data they are now asking for. Unfortunately, we learned that while the attacker's iPhone was in FBI custody the Apple ID password associated with the phone was changed. Changing this password meant the phone could no longer access iCloud services.

As the government has confirmed, we’ve handed over all the data we have, including a backup of the iPhone in question. But now they have asked us for information we simply do not have.

What should happen from here?

Our country has always been strongest when we come together. We feel the best way forward would be for the government to withdraw its demands under the All Writs Act and, as some in Congress have proposed, form a commission or other panel of experts on intelligence, technology, and civil liberties to discuss the implications for law enforcement, national security, privacy, and personal freedoms. Apple would gladly participate in such an effort.

Read Tim's letter

Shop and Learn
Mac
iPad
iPhone
Watch
TV
Music
iTunes
iPod
Accessories
Gift Cards

Apple Store
Find a Store
Genius Bar
Workshops and Learning
Youth Programs
Apple Store App
Refurbished
Financing
Reuse and Recycling
Order Status
Shopping Help

For Education
Apple and Education
Shop for College

For Business
iPhone in Business
iPad in Business
Mac in Business
Shop for Your Business

Account
Manage Your Apple ID
Apple Store Account
iCloud.com

Apple Values
Environment
Supplier Responsibility
Accessibility
Privacy
Inclusion and Diversity
Education

About Apple
Apple Info
Job Opportunities
Press Info
Investors
Events
Hot News
Legal
Contact Apple

More ways to shop: Visit an Apple Store, call 1-800-MY-APPLE, or find a reseller.

Privacy Policy | Terms of Use | Sales and Refunds | Site Map United States

Exhibit 15

The New York Times

TECHNOLOGY

Apple Is Said to Be Trying to Make It Harder to Hack iPhones

By MATT APUZZO and KATIE BENNER FEB. 24, 2016

New York police officers stood guard during a demonstration outside the Apple store on Fifth Avenue on Tuesday.

Jewel Samad/Agence France-Presse — Getty Images

WASHINGTON — Apple engineers have begun developing new security measures that would make it impossible for the government to break into a locked iPhone using methods similar to those now at the center of a court fight in California, according to people close to the company and security experts.

If Apple succeeds in upgrading its security — and experts say it almost surely will — the company will create a significant technical challenge for law enforcement agencies, even if the Obama administration wins its fight over access to data stored on an iPhone used by one of the killers in last year's San Bernardino, Calif., rampage. If the Federal Bureau of Investigation wanted to get into a phone in the future, it would need a new way to do so. That would most likely prompt a new cycle of court fights and, yet again, more technical fixes by Apple.

The only way out of this scenario, experts say, is for Congress to get involved. Federal wiretapping laws require traditional phone carriers to make their data accessible to law enforcement agencies. But tech companies like Apple and Google are not covered, and they have strongly resisted legislation that would place similar requirements on them.

"We are in for an arms race unless and until Congress decides to clarify who has what obligations in situations like this," said Benjamin Wittes, a senior fellow at the Brookings Institution.

Companies have always searched for software bugs and patched holes to keep their code secure from hackers. But since the revelations of government surveillance made by Edward J. Snowden, companies have been retooling their products to protect against government intrusion.

For Apple, security is also a global marketing strategy. New security measures would not only help the company in its fight with the government, but also reassure investors and customers.

"For all of those people who want to have a voice but they're afraid, we are standing up, and we are standing up for our customers because protecting them we view as our job," Apple's chief executive, Timothy D. Cook, said on Wednesday in an interview with ABC News.

Related Coverage

The company first raised the prospect

RELATED COVERAGE

of a security update last week in a phone call with reporters, who asked why the company would allow firmware — the software at the heart of the iPhone — to be modified without requiring a user password.

One senior executive, speaking on the condition of anonymity, replied that it was safe to bet that security would continue to improve. Separately, a person close to the company, who also spoke on the condition of anonymity, confirmed this week that Apple engineers had begun work on a solution even before the San Bernardino attack. A company spokeswoman declined to comment on what she called rumors and speculation.

Independent experts say they have held informal conversations with Apple engineers over the last week about the vulnerability. Exactly how Apple will address the issue is unclear. Security experts who have been studying Apple's phone security say it is technically possible to fix.

"There are probably 50 different ideas we have all sent to Apple," said Jonathan Zdziarski, a security researcher.

Apple built its recent operating systems to protect customer information. As Mr. Cook wrote in a recent letter to customers, "We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."

But there is a catch. Each iPhone has a built-in troubleshooting system that lets the company update the system software without the need for a user to enter a passcode. Apple designed that feature to make it easier to repair malfunctioning phones.

In the San Bernardino case, the F.B.I. wants to exploit that troubleshooting system by forcing Apple to write and install new software that strips away several security features, making it much easier for the government to hack into the phone. The phone in that case is an old model, but experts and former Apple employees say that a similar approach could also be used to alter software on newer phones. That is the vulnerability Apple is working to fix.

Apple regularly publishes security updates and gives credit to researchers who hunt for bugs in the company's software. "Usually, bug reports come in an email saying, 'Dear Apple Security, we've discovered a flaw in your product,' " said Chris Soghoian, a technology analyst with the American Civil Liberties Union. "This bug report has come in the form of a court order."

James B. Comey Jr., director of the F.B.I., said the government is not seeking a skeleton key to iPhones. Drew Angerer for The New York Times

The court order to which Mr. Soghoian referred was issued last week by a federal magistrate, and tells Apple to write and install the code sought by the F.B.I. Apple has promised to challenge that order. Its lawyers have until Friday to file its opposition in court.

In many ways, Apple's response continues a trend that has persisted in Silicon Valley since Mr. Snowden's revelations. Yahoo, for instance, left its email service unencrypted for years. After Mr. Snowden revealed the National Security Agency surveillance, the company quickly announced plans to encrypt email. Google similarly moved to fix a vulnerability that the government was using to hack into company data centers.

Apple's showdown with the Justice Department is different in one important way. Now that the government has tried to force Apple to hack its own code, security officials say, the company must view itself as the vulnerability.

"This is the first time that Apple has been included in their own threat model," Mr. Zdziarski said. "I don't think Apple ever considered becoming a compelled arm of the government."

The F.B.I. director, James B. Comey Jr., signaled this week that he expected Apple to change its security, saying that the phone-cracking tool the government sought in the San Bernardino case was "increasingly obsolete." He said that supported the government's argument that it was not seeking a skeleton key to hack into all iPhones.

Apple, though, says the case could set a precedent for forcing company engineers to write code to help the government break into any iPhone. "The U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create," Mr. Cook said in his letter.

The heated back-and-forth between the government and technology companies is, at least in part, a function of the Obama administration's strategy. The White House has said it will not ask Congress to pass a law requiring tech companies to give the F.B.I. a way to gain access to customer data. That has left the Justice Department to fight for access one phone at a time, in court cases that often go unnoticed.

While it is generally accepted that Silicon Valley's tech giants can outgun the government in a technical fight, the companies do face one important limitation. Security features often come at the expense of making products slower or clunkier.

Apple's brand is built around creating products that are sleek and intuitive. A security solution that defeats the F.B.I. is unworkable if it frustrates consumers. One of the impediments to encrypting all the data in Apple's iCloud servers, for instance, has been finding a way to ensure that customers can easily retrieve and recover photos and other information stored there.

"Telling a member of the public that they're going to lose all the family photos they've ever taken because they forgot their password is a really tough sell," Mr. Soghoian said. "A company wants to sell products to the public."

Matt Apuzzo reported from Washington and Katie Benner from San Francisco.

Follow The New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on February 25, 2016, on page A1 of the New York edition with the headline: Security 'Arms Race' as Apple Is Said to Harden iPhone Tech. Order Reprints | Today's Paper | Subscribe

Exhibit 16

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT

No. 15 MISC 1902 (JO)

APPLE INC.'S RESPONSE TO COURT'S OCTOBER 9, 2015 MEMORANDUM AND ORDER

INTRODUCTION

This Court asked for Apple's views on whether the assistance the government seeks from Apple is technically feasible and, if so, whether compliance with the proposed order would be unduly burdensome. But the Court has also raised an important question of first impression—does the government have the ability to use the All Writs Act to compel a provider of consumer electronic devices like Apple to assist law enforcement in its investigative efforts? This question is particularly timely because social awareness of issues relating to privacy and security, and the authority of government to access data is at an all-time high. And public expectations about the obligations of companies like Apple to minimize government access within the bounds of the law have changed dramatically. Apple acknowledges the basis for this Court's concern that the All Writs Act may not be sufficient authority to require a device manufacturer like Apple to take possession of a device in the government's custody and perform expert forensic services on that device[1] but, as requested by the Court, Apple will limit its response to the topics of feasibility and burden.[2]

FEASIBILITY AND BURDEN OF THE GOVERNMENT'S REQUEST

In most cases now and in the future, the government's requested order would be substantially burdensome, as it would be impossible to perform. For devices running iOS 8 or higher, Apple would not have the technical ability to do what the government requests—take possession of a password protected device from the government and extract unencrypted user

[1] The All Writs Act may not apply here because, among other reasons, the bounds of mandatory law enforcement assistance have already been drawn by the Communications Assistance for Law Enforcement Act (CALEA) and because Apple does not own or control the device in question.

[2] Apple is not requesting oral argument.

data from that device for the government. Among the security features in iOS 8 is a feature that prevents anyone without the device's passcode from accessing the device's encrypted data. This includes Apple.

A more detailed explanation of Apple's security features for iOS 8 and higher can be found in Apple's iOS Security Guide. *See, e.g.*, *iOS Security—White Paper*, Apple Inc. (September 2015), https://www.apple.com/business/docs/iOS_Security_Guide.pdf (last visited Oct. 19, 2015). But at a high level, as relevant here, each Apple device includes both hardware and software security features. For example, each device is provisioned during fabrication with its own Unique ID ("UID") that is not accessible to other parts of the system and is not known to Apple. *Id.* at 10-12. When a user sets up a device passcode, that passcode becomes entangled with the device's UID. *Id.* The passcode thus becomes part of the key-management protections for files encrypted with certain classes of protection. *Id.* The stronger the user passcode is, the stronger the encryption becomes. In iOS 8, the default class of protection changed, and the encryption keys used for the vast majority of files stored on devices now are protected with a key derived from the user-chosen passcode. *Id.* The end-result is that a person must know the passcode to decrypt the majority of the data on the device. This combination of hardware and software security features helps protect users from attackers if Apple's servers are compromised or if the user no longer has physical possession of his or her device. As measured by Apple's App Store, as of October 5, 2015, 90% of Apple's devices are using iOS 8 or higher. *See Support: App Store*, Apple Developer, https://developer.apple.com/support/app-store/ (last visited Oct. 19, 2015).

Here, however, the case involves an Apple device running a version of iOS 7. Such operating system versions are becoming rare as they compromise less than 10% of the devices in the U.S. For these devices, Apple has the technical ability to extract certain categories of unencrypted data from a passcode locked iOS device.[3] Whether the extraction can be performed successfully depends on the device itself, and whether it is in good working order. As a general matter, however, certain user-generated active files on an iOS device that are contained in Apple's native apps can be extracted. Apple cannot, however, extract email, calendar entries, or any third-party app data.

Apple has not inspected the device that is the subject of the government's application so Apple cannot say with certainty that it can extract the requested data. Nor can Apple say with certainty what the burden would be to perform such an extraction assuming it is possible. But the act of extracting data from a single device in good working order, running an operating system earlier than iOS 8, would not likely place a substantial financial or resource burden on Apple by itself. But it is not a matter of simply taking receipt of the device and plugging it into a computer. Each extraction diverts man hours and hardware and software from Apple's normal business operations. And, of course, this burden increases as the number of government requests increases.

Moreover, as the Court recognized in its Memorandum and Order, there may be burdens to Apple beyond "the physical demands and immediate monetary costs of compliance." Oct. 9, 2015 Mem. and Order at 9 (ECF No. 2). The first is the inevitable testimonial demands that will follow such extraction. Once Apple engineers participate in the process, they may be required to testify at trial. *See, e.g.*, *U.S. v. Cameron*, 699 F.3d 621, 643-44, 49 (1st Cir. 2012) (holding that

[3] Apple has previously been ordered to extract data from devices running iOS 7 or earlier and has performed such extractions. These orders generally come in the body of search warrants and contain specific language to avoid confusion over the scope and legitimacy of the demand on Apple. This case marks the first time a judge has questioned the authority of the All Writs Act to grant supplemental orders to accompany such warrants and asked Apple for its views on the feasibility and burden associated with such an order before issuing it.

because child pornography reports generated by Internet provider were testimonial, the reports "should not have been admitted without giving [defendant] the opportunity to cross-examine the [provider] employees who prepared the [reports].") Again, in a single case, that burden may be manageable, but on any significant scale it can be demanding and personnel-intensive. This is not a case where Apple engineers are fact witnesses, required to testify when called. Their involvement in any proceedings would be solely due to their mandated service under the proposed order.

Second, public sensitivity to issues regarding digital privacy and security is at an unprecedented level. This is true not only with respect to illegal hacking by criminals but also in the area of government access—both disclosed and covert. Apple has taken a leadership role in the protection of its customers' personal data against any form of improper access. Forcing Apple to extract data in this case, absent clear legal authority to do so, could threaten the trust between Apple and its customers and substantially tarnish the Apple brand. This reputational harm could have a longer term economic impact beyond the mere cost of performing the single extraction at issue.

CONCLUSION

The questions this Court raised in its Memorandum and Order are both vital and timely. Application of the All Writs Act in this case imposes a real burden on Apple—commercial and reputational. Should the Court determine that the law does not support the government's reliance on the All Writs Act for the reasons the Court identified, Apple respectfully requests that the Court deny the government's application for an order requiring Apple to perform extraction services on the Apple-manufactured device in the government's custody.

Dated: October 19, 2015

Respectfully submitted,

/s/ Ken Dreifach
Ken Dreifach (Bar No. KD4816)
ZwillGen PLLC
232 Madison Avenue
New York, NY 10016
(646) 362-5590

Marc Zwillinger (*pro hac vice*)
Jeffrey Landis (*pro hac vice*)
ZwillGen PLLC
1900 M Street, NW, Suite 250
Washington, DC 20036
(202) 296-3585

Counsel for Apple Inc.

CERTIFICATE OF SERVICE

I hereby certify that on October 19, 2015, the foregoing document was filed with the Clerk of the Court and served in accordance with the Federal Rules of Civil Procedure, the Eastern District's Local Rules, and the Eastern District's Rules on Electronic Service upon the following parties and participants:

Lauren Howard Elbert
Assistant United States Attorney
Eastern District of New York
271 Cadman Plaza East
Brooklyn, NY 11201
(718) 254-7577

/s/ Jeffrey Landis
Jeffrey Landis (*pro hac vice*)
ZwillGen PLLC
1900 M Street, NW, Suite 250
Washington, DC 20036
(202) 296-3585

EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Chief, Cyber and Intellectual Property Crimes Section
Assistant United States Attorney
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2400
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)

SUPPLEMENTAL DECLARATION OF CHRISTOPHER PLUHAR IN SUPPORT OF GOVERNMENT'S REPLY IN SUPPORT OF MOTION TO COMPEL AND OPPOSITION TO APPLE INC.'S MOTION TO VACATE ORDER

Hearing Date: March 22, 2016
Hearing Time: 1:00 p.m.
Location: Courtroom of the Hon. Sheri Pym

SUPPLEMENTAL DECLARATION OF CHRISTOPHER PLUHAR

I, Christopher Pluhar, declare and state as follows:

1. I am a Supervisory Special Agent ("SSA") with the FBI, and I have knowledge of the facts set forth herein and could and would testify to those facts fully and truthfully if called and sworn as a witness.

A. The Subject Device Was Off When Seized

2. In paragraph 8 of my declaration dated February 16, 2016 (the "Initial Declaration"), I explained that the Subject Device was "locked" because it presented a numerical keypad with a prompt for four digits. To add further detail, on December 3, 2015, the same day the Subject Device was seized from the Lexus IS300, I supervised my Orange County Regional Computer Forensics Laboratory ("OCRCFL") team who performed the initial triage of the Subject Device, and observed that the device was powered off, and had to be powered up, or booted, to conduct the triage. Upon power-up, we observed that the device was protected with a four-digit passcode (because it displayed a number pad with four spaces), and was running iOS9. I confirmed with two FBI Evidence Response Team agents that the device was found in the center console of the Lexus IS300 described in the search warrant, and that it was found there powered off.

B. Accessing the iCloud Back-Ups

3. As described in paragraphs 5 and 6 of my Initial Declaration, after the shootout on December 2, 2016, the Subject Device was seized pursuant to the search warrant on December 3, 2016. After case agents and forensic examiners from the OCRCFL met with personnel (including Information Technology ("IT") personnel) from the San Bernardino County Department of Public Health ("SBCDPH"), I then met personally on December 6, 2015 with IT specialists at the SBCDPH to gather more information about the Subject Device and the SBCDPH account(s) associated with the Subject Device. I learned from SBCDPH personnel that the department had deployed a mobile device management ("MDM") system to manage its recently issued fleet of iPhones, that the MDM system had not yet been fully implemented, and that the

necessary MDM iOS application to provide remote administrative access had not been installed on the Subject Device. As a result, SBCDPH was not able to provide a method to gain physical access to the Subject Device without Farook's passcode.

4. As described in paragraph 7 of my Initial Declaration, the Subject Device is owned by SBCDPH. I learned from SBCDPH IT personnel that SBCDPH also owned the iCloud account associated with the Subject Device, that SBCDPH did not have the current user password associated with the iCloud account, but that SBCDPH did have the ability to reset the iCloud account password.

5. Without the Subject Device's passcode to gain access to the data on the Subject Device, accessing the information stored in the iCloud account associated with the Subject Device was the best and most expedient option to obtain at least some data associated with the Subject Device. With control of the iCloud account, the iCloud back-ups of the Subject Device could be restored onto different, exemplar iPhones, which could then be processed and analyzed.

a. As described in Apple's security documentation, a "passcode" is a component of the encryption key that protects the device itself, which is distinct from the "password" associated with an Apple ID needed to access Apple's Internet Services, such as iCloud. *See* Apple's iOS Security for iOS 9.0 (Sept. 2015) ("iOS Security") attached to the Declaration of Nicola T. Hanna as Exhibit K; *id.* at 11-12 (describing passcode's role in creating device's class key); *id.* at 38 (describing different password requirements for Apple ID needed for Apple's Internet Services); *id.* at 41 ("Users set up iCloud by signing in with an Apple ID"). Each iCloud account is associated with a specific Apple ID.

b. Therefore the pass*word* necessary to access the iCloud account associated with the Subject Device is unrelated to the pass*code* needed for physical access to the Subject Device itself.

6. While in discussions with SBCDPH IT personnel, I also spoke with Lisa Olle, attorney for Apple Inc. Ms. Olle provided me various pieces of useful information

about the iCloud account associated with the Subject Device, including information about the existing back-ups, confirmation that the entire iCloud account had already been preserved by Apple in response to an FBI request for preservation, and that the remote-wipe function was not activated for the Subject Device. Ms. Olle advised that once the search warrant was received by Apple, there would be an unknown time delay for Apple to provide the Subject Device iCloud account data.

7. After that conversation with Ms. Olle, and after discussions with my colleagues, on December 6, 2015, SBCDPH IT personnel, under my direction, changed the password to the iCloud account that had been linked to the Subject Device. Once that was complete, SBCDPH provided exemplar iPhones that were used as restore targets for two iCloud back-ups in the Subject Device's iCloud account. Changing the iCloud password allowed the FBI and SBCDPH IT to restore the contents of the oldest and most recent back-ups of the Subject Device to the exemplar iPhones on December 6, 2015. Once back-ups were restored, OCRCFL examiners processed the exemplar iPhones and provided the extracted data to the investigative team. Because not all of the data on an iPhone is captured in an iCloud back-up (as discussed further below), the exemplar iPhones contained only that subset of data as previously backed-up from the Subject Device to the iCloud account, not all data that would be available by extracting data directly from the Subject Device (a "physical device extraction").

C. Not All Data on an iPhone is Backed Up to the iCloud

8. Subsequently, a search warrant was issued on January 22, 2016, to obtain the preserved contents of the Apple ID and iCloud account associated with the Subject Device. Review of the iCloud search warrant results that were received from Apple on January 26, 2016 is ongoing, but review of this data is difficult compared to the data restored to the exemplar iPhones due to the manner in which it has been formatted and delivered by Apple.

9. The results of the iCloud search warrant confirm that the last Subject Device back-up to the iCloud account was on October 19, 2015 (approximately 6 weeks

before the December 2, 2015 attack in San Bernardino), as stated in paragraph 8 of my Initial Declaration. According to the logs contained in those results, on October 22, 2015, it appears that the "iForgot" web-based password change feature was used for the account associated with the Subject Device. I know based on my experience, and review of Apple's website, that "iforgot.apple.com" provides iCloud customers with the ability to reset the password associated with their iCloud account over the Internet.

10. Regarding iCloud back-ups, I know from training and experience as a mobile device forensic examiner, and consultation with other FBI technical experts that, in general, cloud-based back-ups of physical devices contain only a subset of the data that is typically obtained through physical device extractions.

a. For example, with iCloud back-ups of iOS devices (such as iPhones or iPads), device-level data, such as the device keyboard cache, typically does not get included in iCloud back-ups but can be obtained through extraction of data from the physical device. The keyboard cache, as one example, contains a list of recent keystrokes typed by the user on the touchscreen. From my training and my own experience, I know that data found in such areas can be critical to investigations.

b. I also know that the Apple iOS allows users to change settings on the device to exclude certain apps from including their user data in iCloud back-ups, but the user data associated with apps excluded from iCloud back-ups by the user may still be obtained via physical device extraction.[1] I consulted with an OCRCFL examiner who reviewed the exemplar iPhones that were used as restore targets for the iCloud back-ups of the Subject Device. Each of the restored exemplars includes restored settings, and those settings showed that, for example, iCloud back-ups for "Mail," "Photos," and "Notes" were all turned off on the Subject Device.

11. For these reasons, iCloud back-ups as currently implemented are not

[1] I also know that developers of iOS apps have the ability to design their apps to specifically exclude app user data from iCloud back-ups, but the user data associated with those apps may still be obtained via physical device extraction.

considered a comprehensive method of extracting all available stored data from an iOS device. For iOS devices, as well as other mobile device platforms, back-ups such as those made to iCloud can provide valuable evidence, but forensic examiners rely on physical device extractions to obtain the most data available from mobile devices. Therefore, even if it had been possible, via any means, to initiate a fresh iCloud back-up of the Subject Device, so that it included information through December 2, 2015, the FBI would still need to conduct a physical device extraction of the Subject Device in order to obtain all potential evidence from the Subject Device.

12. Before seeking the February 16, 2016, Order, in a phone conversation of which I was a part, the government explained to Lisa Olle and Erik Neuenschwander, among others from Apple, in detail its proposal for technical assistance including specifics of the three desired functions and how they might be achieved as embodied in the Order. After hearing the government's proposal, the Apple representatives declined to discuss the feasibility of the government's proposal and instead provided a list of alternative ways the government might be able to access some of the data on the Subject Device. Although the FBI had already explored these avenues, I, and others from the technical team re-explored them at the suggestion of Apple representatives. We again determined that none provided any means to access the full set of data on the Subject Device. In a subsequent phone conversation with Erik Neuenschwander and Lisa Olle, we explained that the alternatives they had suggested did not work. Erik Neuenschwander and Lisa Olle declined to discuss the feasibility of the government's proposal as embodied in the Order.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that this declaration is executed at California, on March 9, 2016.

Christopher Pluhar
Supervisory Special Agent
Federal Bureau of Investigation

EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Chief, Cyber and Intellectual Property Crimes Section
Assistant United States Attorney
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-2400
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE #5KGD203

ED No. CM 16-10 (SP)

DECLARATION OF STACEY PERINO IN SUPPORT OF GOVERNMENT'S REPLY IN SUPPORT OF MOTION TO COMPEL AND OPPOSITION TO APPLE INC.'S MOTION TO VACATE ORDER; EXHIBITS 17-30

Hearing Date: March 22, 2016
Hearing Time: 1:00 p.m.
Location: Courtroom of the Hon. Sheri Pym

DECLARATION OF STACEY PERINO

I, Stacey Perino, declare as follows:

1. I am an Electronics Engineer with the Federal Bureau of Investigation ("FBI"). I have knowledge of the facts set forth herein and could and would testify to those facts fully and truthfully if called and sworn as a witness.

2. I received a Bachelor of Science in Mechanical Engineering from Colorado State University in 1991. I received a Bachelor of Science Degree in Electrical Engineering from the University of Colorado in 1996. I have been employed as an Electronics Engineer with the Federal Bureau of Investigation since 1996. From 1996 to 2001, I was an electrical engineer in the FBI's Cryptologic and Electronic Analysis Unit ("CEAU") developing both hardware and software solutions to recover data from electronic devices. From 2001 to 2009, I was the Program Manager for the Embedded Engineering Program within that same unit in the FBI. During this time I managed the technical efforts for a team of electrical engineers, computer engineers and computer scientists, composed of both government and contractor personnel with a focus on the recovery and presentation of data from electronic devices. In 2009, I became the Technical Director of the CEAU, a position I still hold.

3. This declaration is made in support of an application seeking an order from the Court compelling Apple Inc. ("Apple") to assist the FBI in its effort to search a cellular telephone, Apple make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ, IMEI:358820052301412, on the Verizon Network ("Subject Device").

4. In addition to relying on my own education, training, and experience, in preparing this declaration, I have reviewed the following:

a. The Declarations of Christopher Pluhar dated February 16, 2016 ("Initial Pluhar Declaration") and March 9, 2016, the Application filed in Case No. 16-

10 in the Central District of California, and the Court's Order in the same case calling for a software image file or "SIF" to be prepared by Apple (the "Order").

b. The Declaration of Erik Neuenschwander dated February 25, 2016 ("Neuenschwander Declaration").

c. Apple's "iOS Security" for iOS 9.0 or later dated September 2015 ("iOS Security"), attached to the Declaration of Nicola T. Hanna as Exhibit K.

d. Documentation from the website of the information technology company Sogeti, attached hereto as Exhibit 17, available at http://esec-lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf.

e. The repository of code stored at https://code.google.com/archive/p/iphone-dataprotection, described as "ios forensics tools," and "Tools and information on iOS 3/4/5/6/7 data protection features."

f. Cellebrite Physical Extraction Manual for iPhone & iPad (Rev 1.3), attached hereto as Exhibit 18.

g. Apple's "Cryptographic Services," attached hereto as Exhibit 19, available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/Security_Overview/CryptographicServices/CryptographicServices.html.

h. Materials from Apple's "Code Signing Guide":

i. Exhibit 20, "About Code Signing," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/Introduction/Introduction.html.

ii. Exhibit 21, "Code Signing Overview," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/AboutCS/AboutCS.html.

iii. Exhibit 22, "Code Signing Tasks," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/Procedures/Procedures.html.

iv. Exhibit 23, "Code Signing Requirement Language," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/CodeSigningGuide/RequirementLang/RequirementLang.html.

i. Materials from Apple's "Cryptographic Services Guide":

i. Exhibit 24, "About Cryptographic Services," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Introduction/Introduction.html.

ii. Exhibit 25, "Cryptography Concepts In Depth," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/CryptographyConcepts/CryptographyConcepts.html.

iii. Exhibit 26, "Encrypting and Hashing Data," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/GeneralPurposeCrypto/GeneralPurposeCrypto.html.

iv. Exhibit 27, "Managing Keys, Certificates, and Passwords," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/KeyManagementAPIs/KeyManagementAPIs.html.

v. Exhibit 28, "Glossary," available at https://developer.apple.com/library/mac/documentation/Security/Conceptual/cryptoservices/Glossary/Glossary.html.

j. Apple's "Unauthorized Modification of iOS Can Cause Security Vulnerabilities, Instability, Shortened Battery Life, and Other Issues," attached hereto as Exhibit 29, and available at https://support.apple.com/en-us/HT201954.

k. Apple's "Code Signing," attached hereto as Exhibit 30, and available at https://developer.apple.com/support/code-signing/.

5. This Declaration relies on Apple's publicly disseminated descriptions of how its own devices, operating system, security features, and software operate. Apple's source code is not, however, publicly available. Therefore the descriptions below do not

rely on my having reviewed Apple's source code, rather they rely upon Apple's own description of its devices, operating system, security features, and software, as well as on my training and experience in both observing and/or conducting the tests described in this document, directing the CEAU embedded engineering analysis of Apple devices and software, and reviewing other open source materials describing Apple mobile device technologies.

A. Purpose of this Declaration

6. In this declaration, I discuss the following topics:

a. The SIF called for in the Order could run *only* on the Subject Device. To explain this, I first provide some background on public key cryptography (Part B.1) and Apple's use of it and code signing to prevent the use of unauthorized code on its products (Part B.2). The Order provides that the SIF would only run on the Subject Device. Apple already requires that iOS updates include a unique device identifier for the Subject Device (Part B.3). Because an iPhone requires Apple to have cryptographically "signed" code before an iPhone will run it, and changing a unique device identifier within the SIF would invalidate Apple's signature, the SIF would not run on other iPhones. (Part B.3.)

b. The SIF called for by the Court's Order would perform functions that already exist in open source software for older devices and operating systems. In other words, code already exists that will bypass the auto-erase and time-delay functions and permit electronic submission of passcodes, but would need to be updated and modified for newer operating systems. (Part C.) That software, however, cannot run on the Subject Device without Apple's "signature."

c. The data contained on the Subject Device can be decrypted *only* on the Subject Device. This is because the encryption key includes a unique identifier that exists only on the Subject Device. (Part D.) Because the decryption must occur on the Subject Device, and because only Apple-signed software can run on the Subject Device

(Part B.2), any code or software tools needed to assist in testing passcodes (even code that includes components that already exist, Part C) must be signed by Apple.

d. Because the Subject Device was powered off when it was seized, it was not possible for it to back itself up to iCloud without the passcode. (Part E.)

B. The SIF Called for by the Order Would Run Only on the Subject Device

1. General Background on Public Key Cryptography

7. Generally, encryption and decryption are the processes of first converting intelligible "plaintext" into unintelligible "ciphertext," and second converting the ciphertext back into plaintext, respectively.

8. While encryption is designed to protect the confidentiality of information, a separate issue that arises in cryptology is authentication. Public key cryptography provides a method to both send messages securely, even when using a non-secure channel, and to validate the messages that are received. A properly implemented cryptographic signature gives the receiver reason to believe the message was sent by the person claiming to be the sender. A cryptographic signature also prevents modification of the original message by anyone other than the signer.

9. Public key encryption uses a complex operation that involves two different keys, a public key and a private key. A public key cryptosystem uses one key to encrypt (or to sign) a message and a different key to decrypt (or verify) the same message. (For this reason it is also referred to as asymmetric.) One of the essential properties of a public key cryptosystem is that it is too difficult—computationally infeasible—to determine a person's private key knowing only that person's public key.

10. The public key is made globally available while the private key is kept confidential. This allows anyone who is a member of the system to use the "phone book" of public keys to send a private message to any other member using the recipient's public key, but it allows only the recipient to open it using that person's private key.

Each key pair is unique to an individual member of a properly implemented cryptosystem.

11. One of the other essential properties of a public key cryptosystem is that the encryption operation and the decryption operation used in the cryptosystem are inverse operations.[1] This means that if one started with a message, it would not matter if one used the encryption operation followed by the decryption operation, or the decryption operation followed by the encryption operation, either would yield the original message again.[2]

12. A more detailed example of how the public key cryptosystem works to sign a message is as follows:

a. Alice generates a public-private key pair, and publishes her public key.

b. Alice composes a Message to Bob, and uses her private key to compute or generate the Signature. (This is represented: Signature = D_{pri}(Message) , where D is the decryption operation.)

c. Alice sends Bob both the Message and the Signature.

d. Bob then uses Alice's public key to verify that the message was signed using her private key. Bob does this by running the inverse "encryption" operation on the Signature. (This is represented: E_{pub}(Signature) = Message, where E is the encryption operation.) If the result of that operation is the Message that Alice sent Bob, then Bob knows the message is not a forgery and came from Alice.

[1] This is represented as follows, where E() and D() denote the encryption and decryption operations, and M is the text of the message: M = E(D(M)) = D(E(M)).

[2] (*See* Ex. 19 at 2, diagram (Apple developer website, Cryptographic Services). *See generally* Ex. 25 at 5, 7 (Apple developer website, Cryptographic Concepts in Depth).)

e. In this example, Alice could also have encrypted the message using Bob's public key. Bob could then have decrypted the message using Bob's own private key.

2. Apple's Use of Public Key Encryption to Prevent the Use of Unauthorized Code on Its Products

13. Just as a cryptosystem can be used to "sign" messages, it can be used to "sign" executable code.[3] Specifically, a vendor can embed a public key into a device such that the public key cannot be altered. For any and all executable code modules, the vendor uses its private key to calculate and attach a signature. As the device loads code modules for execution, the device uses the embedded public key to calculate the signature and thus verify the module's integrity and authenticity. As long as the public key cryptosystem is unbroken and the embedded key cannot be modified within the device, the scheme guarantees that only code issued by the vendor (that has been cryptographically signed) will run on the device.

14. Apple implements this system to require that its devices use software that only Apple authorizes. Apple does this by programming the public key into Read Only Memory ("ROM"). ROM is hardwired during the manufacture of the semiconductor device and cannot be changed later through any software means. The firmware in ROM is the first code that executes on the processor when power is applied. According to Apple's Security documentation, Apple products have also stored "the Apple Root CA [certificate authority] public key" within boot ROM.[4] (iOS Security at 5.) The boot ROM code uses the public key to verify that the next code to load (which is stored in

[3] In simplified terms, software is generally written by programmers in "source code." That source code is converted (or "compiled") into what is referred to as "executable code" that is in a format that a computer processer can understand and "execute."

[4] Boot ROM is firmware that has been fused or hardwired into the processor during manufacturing. It cannot be changed.

memory outside the processor) has also been signed with Apple's private key. (iOS Security at 5.)

15. This system ensures that Apple controls all code loaded and run on the device from the initial power-on. Apple describes how it has implemented this process in what it refers to as its "Chain of Trust" on pages 5-10 of its iOS Security document, wherein each sequential step needed to boot up the operating system and run application software relies on—and requires—Apple's signature. Specific details include the following:

a. "Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware." (*Id.* at 5.)[5]

b. "The Boot ROM code contains the Apple Root CA [certificate authority] public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel." (*Id.*) A certificate authority is the entity that issues digital

[5] A bootloader is the initial code run on a processor that starts the system's hardware components and peripherals and prepares the hardware for the operating system or higher level code. There may be multiple bootloaders that are executed sequentially at startup. The kernel is the first part of an operating system that loads and is responsible for controlling access to the computer's hardware resources. The kernel generally runs in protected memory to which other parts of the operating system and application code cannot directly read or write. Kernel extensions provide a method for adding or changing functionality of Apple's kernel without recompiling/relinking the source code. A mobile device typically has multiple processors; the application processor running an operating system, such as iOS 9.02, with which the user interacts (via the screen and keyboard), and the baseband processor which handles network communications traffic and protocols. The application processor is responsible for starting (booting) the baseband processor. Therefore, the application processor provides the baseband processor with the code it needs to load and run. Thus, Apple's chain of trust calls for each of these steps to be verified, ensuring that the next steps are authorized by Apple before allowing them to run or execute.

certificates. Certificate authorities create the public/private key pairs, and are responsible for ensuring the security of the private key. Apple has built its own certificate authority and has created its own public/private key pair used in the iPhone. As noted above, the public key is permanently programmed into the ROM of the iPhone, while the private key is controlled and protected by Apple. Because only Apple possesses its private key, only Apple is able to sign software that will be loaded on its devices. By keeping the private key secret, Apple ensures that only software signed by Apple using its private key can be loaded on its devices during the boot process.

c. "This secure boot chain helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices." (*Id.*) "From initial boot-up to iOS software updates to third-party apps, each step is analyzed and vetted to help ensure that the hardware and software are performing optimally together and using resources properly." (*Id.*)

d. "This architecture is central to security in iOS, and never gets in the way of device usability. The tight integration of hardware and software on iOS devices ensures that each component of the system is trusted, and validates the system as a whole." (*Id.*)

16. "The startup process described above helps ensure that only Apple-signed code can be installed on a device." (*Id.* at 6.) If any component can be made to load code not signed by Apple, the chain of trust is broken. By beginning their chain of trust with the initial code and public key programmed into the device ROM, Apple has made it extremely difficult for anyone to defeat the chain of trust.

17. As a result of these features, an Apple iPhone is designed to only run code (the operating system and the many pieces of firmware and software that may operate within it) that are signed using Apple's keys.

3. Apple "Signs" iOS Updates for Its iPhones that Include a Unique Device Identifier, Ensuring It Only Works on One iPhone

18. While the features described above permit Apple to ensure that the devices it manufactures will use only an operating system or software that Apple has authorized (by signing it), Apple also relies on them to ensure that an operating system will work only on one specific Apple device. Specifically, during an iOS update, recovery, or Device Firmware Update (DFU) process, the device verifies that the code being loaded to it was digitally signed specifically for that device, and not for another device. This feature, enforced by the hardware-based chain of trust, allows Apple to ensure that any code loaded to the phone will only operate on a specific device.

19. Apple implements this process in the following manner. First, the device connects to a computer, for example through iTunes, and provides iTunes with unique information about itself—both its hardware and software. Second, iTunes sends this information from the device to an Apple server that builds the package of code needed to update or recover that device, packages it with the same unique information about the device, and returns it to the computer running iTunes. Third, upon receiving that package from the computer running iTunes, the device is required to read and recognize its own unique information before installing the operating system.

20. Details of this process are as follows:

a. Apple maintains what it refers to as "the Apple installation authorization server," which is referred to herein as the "Installation Server." (iOS Security at 6.)

b. Whenever a device tries to upgrade its version of iOS, through the upgrade or recovery process, the device must first send to that server a set of information from the device. The information sent by the device includes "cryptographic measurements for each part of the bundle to be installed (for example, LLB, iBoot, the kernel, and OS image)." (*Id.*) Those measurements are a digest or partial digest of that component. (A digest can be a cryptographic hash, or the result of a similar algorithm that generates a unique value, akin to a digital fingerprint, after it processes each part of the bundle.)[6] The device also sends a "nonce," or a random, one-time-use value.

c. Most importantly for ensuring the "personalization" of the software for use on a specific device, the device also sends "the device's unique ID (ECID)." (iOS Security at 6.) The ECID is a unique, device-specific identifier programmed into the phone hardware during manufacture. (*Id.* at 58 (defining ECID as "[a] 64-bit identifier that's unique to the processor in each iOS device. Used as part of the personalization process, it's not considered a secret").) Apple explains the use of these values in their iOS Security document. "These steps ensure that the authorization is for a specific device and that an old iOS version from one device can't be copied to another." (*Id.* at 6.)

d. Once the Apple Installation Server receives this information from the device, it builds a software package and digitally signs it using a private key that is not known to the public. The digital signature includes the ECID, nonce, and other cryptographic measurements in the signed data. Once the device receives the package, the device verifies from the signed data that the package is meant for it.

e. The device is also able to tell that the installation is current and is not a repeat of an older installation (which would result in a "downgrade" of the operating system). The device does so by checking the random, one-time nonce it had sent to the server was the one returned by the server in the signed package. "The nonce prevents an

[6] "In cryptography, hashes are used when verifying the authenticity of a piece of data. Cryptographic hashing algorithms are essentially a form of (extremely) lossy data compression, but they are specifically designed so that two similar pieces of data are unlikely to hash to the same value. . . . . With good hashing algorithms, collisions [messages that hash to the same value] are unlikely if you make small changes to a piece of data. This tamper-resistant nature of good hashes makes them a key component in code signing, message signing, and various other tamper detection schemes." (Ex. 19 at 3 (Apple developer website, Cryptographic Services).) By way of background, data compression that is "lossy" loses some qualities of the original data, such as when a compressed digital image loses resolution or appears "pixelated." In the cryptography context, what is important is that the resulting hash value is unique, not that it be capable of reformulating the entire original piece of data, hence it "loses" data by being reduced to a small but unique string of letters and numbers.

attacker from saving the server's response and using it to tamper with a device or otherwise alter the system software." (*Id.* at 6.)

21. The digital signature prevents any part of the returned package from being changed. If the software in the returned package is altered, the digital signature check will fail and the device will not load it. If the ECID is changed to that of another device, the signature check will fail and the device will not load the code.[7] In other words, unless someone can bypass the digital signature verification, allowing them to load unsigned code, the software cannot be changed to operate on a different device or perform a different function.[8]

22. The Order provides that the SIF would only run on the Subject Device. As shown in the preceding description of Apple's normal code signing process during an iOS update, Apple already has a mechanism in place to do this by including the ECID into the digital signature process. If this same or a similar process were used, the SIF could incorporate the ECID of the Subject Device, and then be signed by Apple. In that case, if the ECID of the SIF were changed to the ECID of another device, the signature check would fail and an Apple device would not load the code.[9]

[7] As described on Apple's developer website: "When a piece of code has been signed, it is possible to determine reliably whether the code has been modified by someone other than the signer." (Ex. 21 at 1 (Apple developer website, Code Signing Overview).) Among the purposes of code signing are to "ensure that a piece of code has not been altered," and to "identify code as coming from a specific source (a developer or signer)." (*Id.*)

[8] Because of the significance of the ability to digitally sign code and therefore cryptographically authenticate it, Apple's developer website explains that a "signing identity, no matter how obtained, is completely compromised if it is ever out of the physical control of whoever is authorized to sign code." (Ex. 22 at 2 (Apple developer website, Code Signing Tasks).)

[9] An additional measure to ensure the SIF would only run on the Subject Device could be to program the Subject Device's ECID directly into the software running in the SIF. In this scenario, the SIF would read the ECID of the device on which it was running, and compare that to the ECID of the Subject Device that had been programmed into it; if the two did not match, the software would exit. In other words, while the iOS update scenario described in this Part relies on the *device's* refusal to run the code without a valid Apple signature (which signature would be invalid by changing the ECID), the *SIF* could refuse to fully execute if it did not detect the Subject Device's

(footnote cont'd on next page)

23. For these reasons, the SIF called for by the Order would be permitted to run only on the Subject Device. In other words, the creation of the SIF, tailored and signed with the unique identifier of the Subject Device, would not undermine the security of other iPhones that also require Apple-signed code, because each iPhone has its own unique identifier. The SIF proposed by the Order would therefore not break Apple's chain of trust on its iPhones, or even on the Subject Device; Apple's assistance will keep the chain of trust intact.

24. Importantly, if somebody were to bypass the Apple digital signature process, the chain of trust would be broken. Causing an Apple device to allow itself to run software not signed by Apple is referred to as "jailbreaking" the device. Jailbreaks result from bugs or errors in different programs that can be exploited to run unsigned code on a device. To my knowledge, for the iPhone 5C, jailbreaks have been exclusively performed from a powered-on phone on which the passcode has been entered and the phone unlocked. Thus there are currently no published jailbreaks for an iPhone 5C where the passcode has not been entered at least once since powering on, and hence there are none that could be applied to the Subject Device.

C. Software Already Exists that Performs Similar Functions as the SIF

25. The security features created and implemented by Apple that are described above were challenged by researchers and hackers as previous iterations of iOS were released. Apple's current chain of trust structure has fixed previous issues, but the methods that have been published and used to test earlier versions of iPhones illustrate why the components used in the SIF already exist, and why it, like other previous tools, can be operated from random access memory ("RAM").

26. Paragraph 19 of the Neuenschwander Declaration states that Apple's "current iPhone operating systems designed for consumer interaction do not run in

ECID. This example is designed to illustrate that there is more than one way to cause the SIF to only load and execute on the Subject Device.

RAM, but are installed on the device itself. To make them run in RAM, Apple would have to make substantial reductions in the size and complexity of the code." As the discussion below illustrates, the SIF would not be designed for "consumer interaction." Rather, the SIF would be designed only to test passcodes, and other similar tools that have previously been used for this purpose do run in RAM.

27. Those previous tools that are available cannot be used on the Subject Device because they are not signed by Apple, and the current chain of trust on the Subject Device requires Apple to have signed any software that will be allowed to run.

28. A more detailed description is as follows:

a. <u>A previous bug allowed a cold-booted[10] iPhone to load a "minimal" operating system in memory (RAMdisk) that had not been signed by Apple.</u> Previously, Apple iPhone versions 3GS and 4 contained a bug in the Apple boot ROM that allowed unsigned code to be loaded and run through Recovery or DFU mode. This vulnerability was published as the "limera1n" exploit. Other researchers analyzed the Apple boot process and published details of it, including the composition of the RAMdisk (*i.e.*, which software components were bundled into the RAMdisk) used in the Recovery mode and DFU mode process to update device firmware.

b. <u>A passcode-recovery tool has already been developed that uses brute-force techniques.</u> The information technology company Sogeti[11] analyzed Apple's encryption process demonstrating that any passcode "guessing" had to be performed by code running on the device and could not be done externally (further explained below in Part D). Other vulnerability researchers used this result to develop software that could brute force the passcode on a jailbroken device (iphone-dataprotection project[12]).

[10] Cold-boot refers to a phone that has been powered off and then powered back on but no passcode has been entered.

[11] (Ex. 17 (http://esec-lab.sogeti.com/static/publications/11-hitbamsterdam-iphonedataprotection.pdf).)

[12] (https://code.google.com/archive/p/iphone-dataprotection, "ios forensics tools," and "Tools and information on iOS 3/4/5/6/7 data protection features.")

c. From this open source research, several forensic tools were developed that combined (1) the boot ROM code signing defeat, and (2) brute-force passcode guessing. Examples include the Cellebrite UFED tool and an FBI-developed tool. Both the Cellebrite[13] and FBI tools utilize the boot ROM exploit, allowing iPhone 3GS and iPhone 4 devices to load and boot an unsigned RAMdisk containing code to brute force the device passcode. The passcode recovery process operated from RAM, and did not alter the system or user data area. The passcode recovery software did not require user interaction, and the entire process ran without use of the "Springboard" graphical user interface. Because these forensic tools ran from a RAMdisk and did not use the operating system that was stored on the device, these tools did not incur time delays or the auto-erase function (which are features implemented by the operating system installed on the device).

d. Apple addressed the bug, and subsequently a jailbreak (*i.e.*, allowing code unsigned by Apple) could only occur on an iPhone after it had been booted and unlocked. As described previously, a jailbroken phone is one that has had the chain of trust broken and can run unsigned code.[14] After Apple corrected the bug present in the

[13] Cellebrite is a private company that makes forensic data recovery tools for mobile devices. While I have not examined the source code for the UFED tool, based on the Cellebrite Physical Extraction Manual for iPhone and iPad (Rev 1.3) and the fact that the Cellebrite tool no longer supports iPhone 4S and later devices, I believe the UFED tool relied on the same ROM exploit. The manual states: "The extraction application does not load iOS but instead loads a special forensic utility to the device. This utility is loaded to the device's memory (RAM) and runs directly from there." The utility is loaded from recovery mode.

[14] The use of jailbroken phones discussed in this Part occurred in a testing environment. Outside of a testing environment, some users have jailbroken their phones to try to use software or services that Apple has not authorized, but Apple cautions that doing so presents "[s]ecurity vulnerabilities": "Jailbreaking your device eliminates security layers designed to protect your personal information and your iOS device. With this security removed from your iOS device, hackers may steal your personal information, damage your device, attack your network, or introduce malware, spyware or viruses." (Ex. 29 (https://support.apple.com/en-us/HT201954).) Furthermore, the jailbreaking process often results in deletion or alteration of data stored on the phone. As discussed in this Part, software already exists that performs certain functions that could be used in the SIF, and to the extent those software components could be used to undermine security, they (like the SIF) would only work on devices that had already assumed security vulnerabilities by being jailbroken.

iPhone 3GS and 4, all known jailbreaks have been applied from within the iPhone user interface, instead of during the boot process. There are publicly known jailbreaks for most recent iPhone OS versions (up to at least version iOS 9.0.2), but they can only be executed from an unlocked iPhone via the user interface, *i.e.*, after the iPhone had booted and had been unlocked. After these jailbreaks are applied, software that has not been signed by Apple may be run.

e. <u>The same brute-force source code still works on jailbroken iPhones.</u> A software project named "iphone-dataprotection" includes a passcode recovery program that can still be compiled, loaded, and run within a jail-broken Apple device. The FBI tool used essentially the same functionality as this project but executed it from a RAMdisk. The FBI recently tested the iphone-dataprotection passcode recovery software on a jailbroken iPhone 6 Plus running iOS 8.4 (in which the passcode had been entered once). With minor modifications this software still functioned and was able to recover the passcode without incurring time delays. The FBI also tested this passcode recovery software on a jailbroken iPad Air 2 running iOS 9.02. In this device the passcode recovery software functioned, but it did incur the time delays and most likely would have erased the device.[15] However, this test does verify that the passcode recovery code works, which has existed for many years and still functions essentially the same. This specific code would not run on the Subject Device "as is," because it is not signed by Apple and also because it would incur time delays and risk causing the device to erase, which would require further development and modifications to the kernel software.[16]

[15] It should be noted that the iPhone 6 and iPad Air 2 both use the more advanced A8 processor and the time delay and erase functionality has moved into a separate security controller called the Secure Enclave.

[16] For example, in previous versions of iOS the time delay and password try count resided in the "springboard" user interface, which is in part what allowed the passcode recovery software to work and to bypass the time-delay and auto-wipe features. In approximately iOS 8.4, that functionality moved from the Springboard and would require further modification to bypass the delay and wipe functions.

f. Only Apple can produce and sign the RAMdisk needed to run the passcode guessing code without first unlocking the iPhone. Beginning with the release of the iPhone 4S in 2011, Apple fixed the bug in the boot ROM. Since that time, the Apple chain of trust—which governs the boot process on an iPhone—has remained intact, preventing loading of unsigned RAMdisks. (The jailbreaks that have occurred on iPhones 5C or later have occurred after the boot-up process has occurred, and after a passcode has been entered; the chain of trust through the boot-up process remains intact on those phones.) However, the steps used in the Apple Recovery and DFU mode boot processes have not changed substantially since that time, and Apple's use of a RAMdisk to perform the updates and device recovery processes appear consistent with the methodology of the earlier devices. Without assistance from Apple to digitally sign the code, however, it has not been possible to continue development of these tools for newer devices. The passcode-guessing software employed by these tools has been tested within jailbroken devices running an iOS that has already been booted and unlocked; neither the FBI, nor others to my knowledge, however, have been able to integrate the software into a RAMdisk to test passcodes from a cold-booted iPhone device since the iPhone 4.

29. As set forth above in the previous paragraph, there are already software components available that perform some of the functions of the SIF called for by the Court's Order. Although code similar to what would be in the SIF already exists, it cannot be used on the Subject Device without Apple's signature because of Apple's robust security and code-signing practices.

D. The Encrypted Data on the Subject Device Must Be Decrypted on the Subject Device Itself

30. As described in paragraph 12 of the Initial Pluhar Declaration, an iPhone 5C running iOS 9 is encrypted using a combination of two components: one user-determined passcode, and one unique 256-bit key (referred to as a "UID") fused into the

phone itself during manufacture. (iOS Security at 12; *id.* 11 (diagram); Neuenschwander Decl. ¶ 13.) These two different components are discussed below.

31. According to Apple's documentation, the UID is unique to each device, is fused into the hardware, and is not known to Apple or anyone else, as described on page 10 of iOS Security:

> The device's unique ID (UID) . . . [is] fused . . . into the application processor and Secure Enclave during manufacturing. No software or firmware can read them directly . . . . The UIDs are unique to each device and are not recorded by Apple or any of its suppliers. . . . The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if the memory chips are physically moved from one device to another, the files are inaccessible. The UID is not related to any other identifier on the device.

32. I know from Supervisory Special Agent ("SSA") Pluhar that the Subject Device was powered off when the FBI found it. When the Subject Device was powered on, it displays a numerical keypad (like that on a telephone), and a prompts for four numbers to be entered.

33. With a four-digit numerical pin, there are only 10,000 possible passcodes. Testing 10,000 passcodes electronically would likely take less than a day, depending on how the SIF were configured.

34. Apple's iOS Security also explains that because its passcodes are permitted to be weak in that they can be only four numbers, Apple has included additional features to discourage brute-force attacks. These features are described in paragraphs 13 and 14 of the Initial Pluhar Declaration, and on page 12 of Apple's iOS Security (noting that iOS 9 iPhones (1) escalate time delays between failed passcodes, and can (2) be configured to wipe their contents after ten failed passcodes, to "discourage brute-force passcode attacks").

35. The UID is itself a strong encryption key. It is fused into the hardware and is both unknowable and unchangeable: it is always used the same way to create the encryption key. The only variable is the passcode.

36. Because both the UID, which is unique and embedded in the device itself, is a part of the encryption key (along with the user-generated passcode), the data that is stored on the Subject Device will need to be decrypted on the Subject Device. Because only Apple-signed software can run on the iPhone, and the decryption must occur on the Subject Device, any code or software tools needed to assist in testing passcodes must be signed using Apple's encryption keys.

E. Apple's iCloud Backup

37. I know from SSA Pluhar that the Subject Device was found in a powered-off state. Based on Apple's published documentation, open source research relating to Apple's encryption, and Apple press releases about iOS 8 and later encryption, I believe that (1) the device would not connect to a WiFi network until the passcode was entered, and (2) even if the device could be forced to perform an iCloud backup, the user data would still be encrypted with the encryption key formed from the 256 bit UID and the user's passcode.

38. Subsequent to seizing the Subject Device, the FBI performed several tests on exemplar phones to test whether a cold-booted iPhone could connect to a trusted WiFi network and perform a backup. The result of that testing was that cold-booted iPhones would not connect to a WiFi network.

a. To the best of my knowledge, a cold-booted iPhone will not connect to WiFi networks trusted by the Subject Device such as a home or work network until the passcode is entered. However, according to Apple and verified by the FBI, there are some WiFi networks inherently trusted by iOS, such as those operated by iPhone sponsors (referred to as carrier-sponsored WiFi). For example, an AT&T iPhone can automatically connect to an AT&T hotspot.

b. When the FBI tested a locked AT&T phone on which the passcode had been entered once by taking it to an area with an AT&T hotspot, the phone connected automatically to the hotspot, as indicated by the WiFi indicator on the top banner of the lock screen display. Additionally the “Find My iPhone” service was used and was able to locate the iPhone, verifying that a phone in which the passcode has been entered will connect, even when screen-locked, to a trusted WiFi network.

c. The same test was also done with the phone first powered off and restarted, but with the passcode not having been entered. In this scenario, the test phone did not show any indication it was connected to the AT&T hotspot through the banner. Additionally, the “Find My iPhone” service was unable to locate the device. The results of these tests show that WiFi is not enabled on the device until after the passcode is entered.

d. Further tests were conducted by myself and a colleague in CEAU by taking an iPhone 5 running iOS 9.02 and an iPhone 6 Plus running iOS 9.2 into a radio-frequency shielded chamber to test their electronic emissions. Both iPhones were fully charged, connected to power and had their WiFi enabled. The same series of tests was done on both phones with identical results. When the iPhone was not protected by a passcode and was powered on in that chamber, it began to emit signals in the frequency band of 2.4 gigahertz (GHz), a common band for WiFi connections. This is consistent with the iPhone trying to detect a WiFi network. When the iPhone *was* protected by a passcode and was powered on in the same chamber without entering the passcode, no emissions in the 2.4 GHz frequency band were detected. This indicates that the WiFi was not active. When the passcode was entered, WiFi 2.4GHz emissions were detected. The phone was allowed to screen lock after the passcode had been entered. Again, 2.4GHz emissions were detected. Each phone was rebooted, no passcode entered, and left overnight in the chamber. No 2.4GHz signals were observed. These tests indicate the WiFi is not active on a cold-booted device until the passcode has been entered at least once.

e. The FBI does not know of any way to force an iPhone that has not had the passcode entered at least once since being powered on to perform an iCloud backup.

39. This result is consistent with Apple's security documentation, which states that data stored on the device is encrypted using a key that is a combination of both the UID (the device-specific unique identifier) and the passcode generated by the user. Unless the passcode is entered by the user, the entire encryption key could not be used to decrypt the data, and the data therefore could not be backed-up to an iCloud—at least in a state that could be recovered outside the device.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that this declaration is executed at Virginia, on March 9, 2016.

Stacey Perino

STACEY PERINO

Exhibit 17

iPhone data protection in depth

Jean-Baptiste Bédrune
Jean Sigwald
Sogeti / ESEC
jean-baptiste.bedrune(at)sogeti.com
jean.sigwald(at)sogeti.com

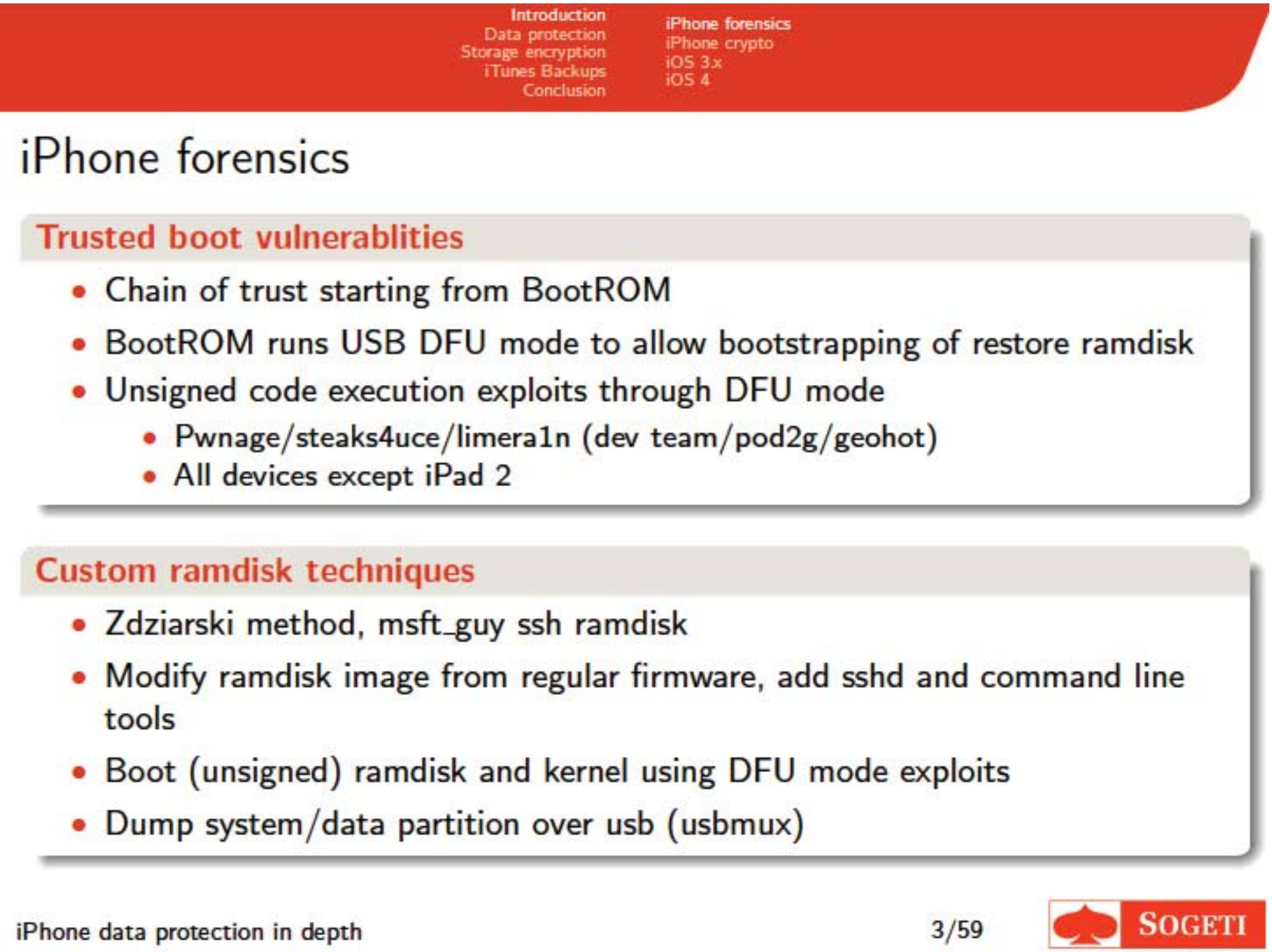
Introduction

Motivation

- Mobile privacy is a growing concern
- iPhone under scrutiny
  - iPhoneTracker (O'Reilly)
  - "Lost iPhone? Lost Passwords!" (Fraunhofer)

Agenda

- iOS 4 data protection
- Storage encryption details
- iTunes backups



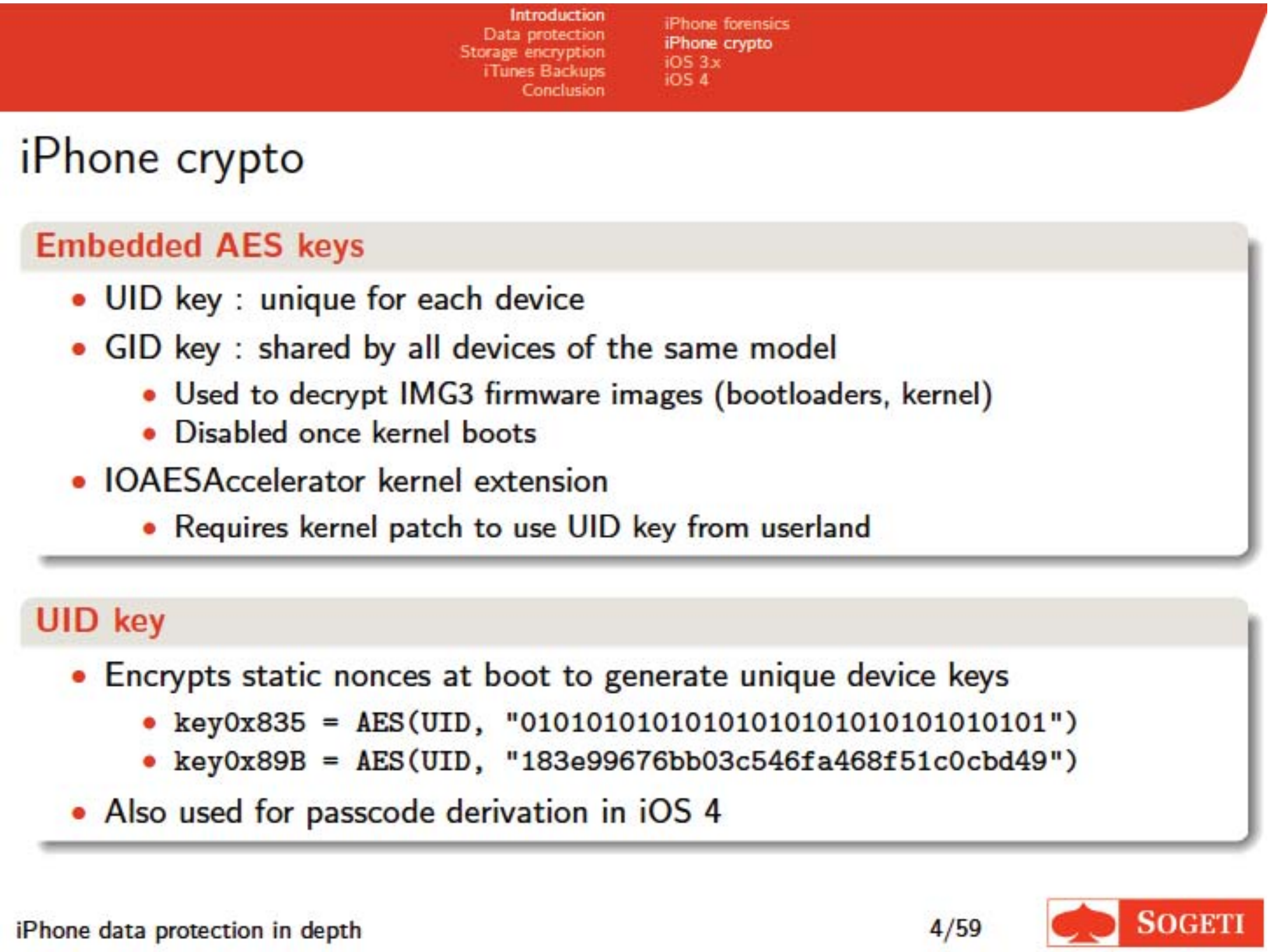
iPhone forensics

Trusted boot vulnerablities

- Chain of trust starting from BootROM
- BootROM runs USB DFU mode to allow bootstrapping of restore ramdisk
- Unsigned code execution exploits through DFU mode
    - Pwnage/steaks4uce/limera1n (dev team/pod2g/geohot)
    - All devices except iPad 2

Custom ramdisk techniques

- Zdziarski method, msft_guy ssh ramdisk
- Modify ramdisk image from regular firmware, add sshd and command line tools
- Boot (unsigned) ramdisk and kernel using DFU mode exploits
- Dump system/data partition over usb (usbmux)



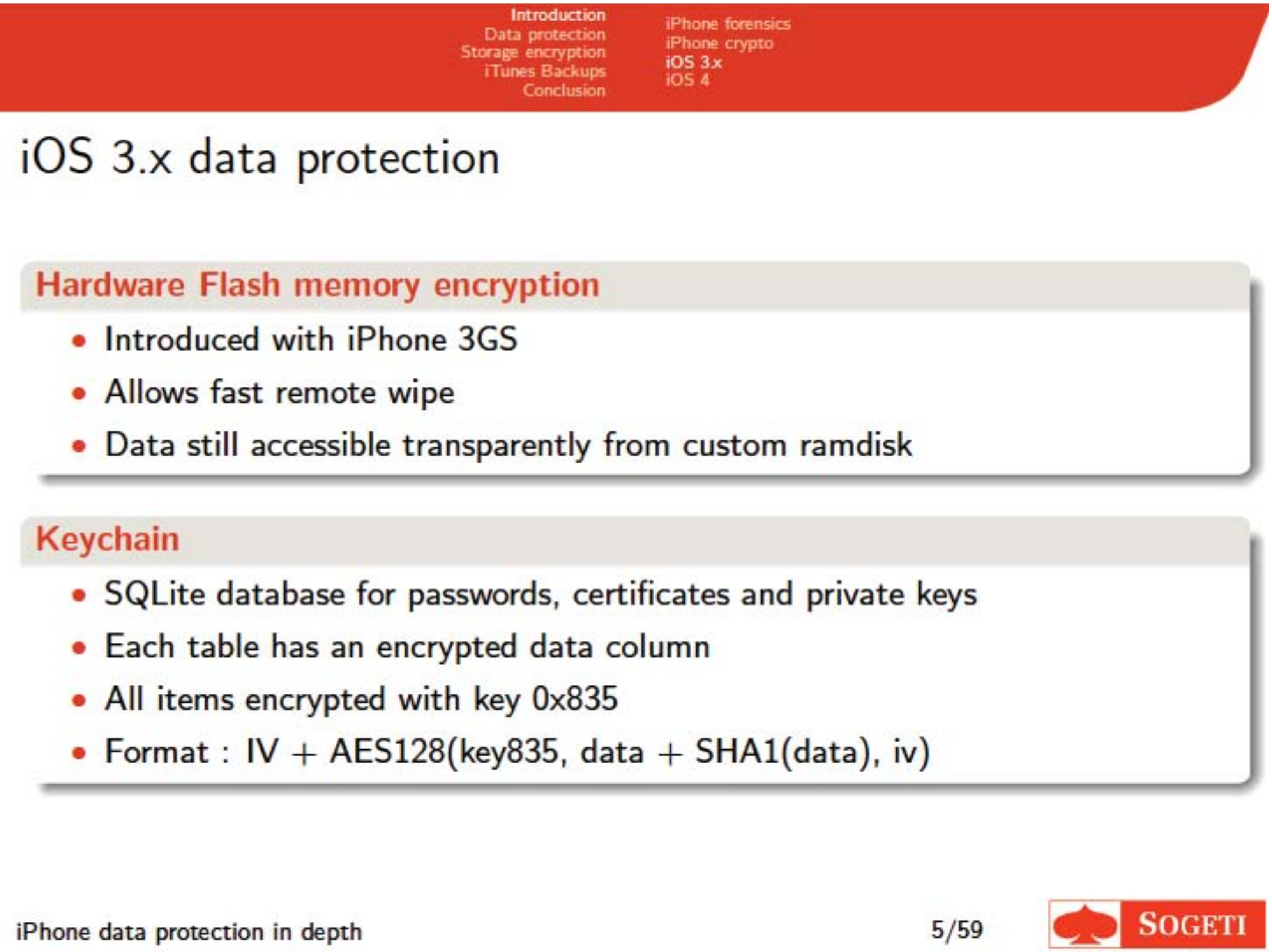
iPhone crypto

Embedded AES keys

- UID key : unique for each device
- GID key : shared by all devices of the same model
  - Used to decrypt IMG3 firmware images (bootloaders, kernel)
  - Disabled once kernel boots
- IOAESAccelerator kernel extension
  - Requires kernel patch to use UID key from userland

UID key

- Encrypts static nonces at boot to generate unique device keys
  - `key0x835 = AES(UID, "01010101010101010101010101010101")`
  - `key0x89B = AES(UID, "183e99676bb03c546fa468f51c0cbd49")`
- Also used for passcode derivation in iOS 4



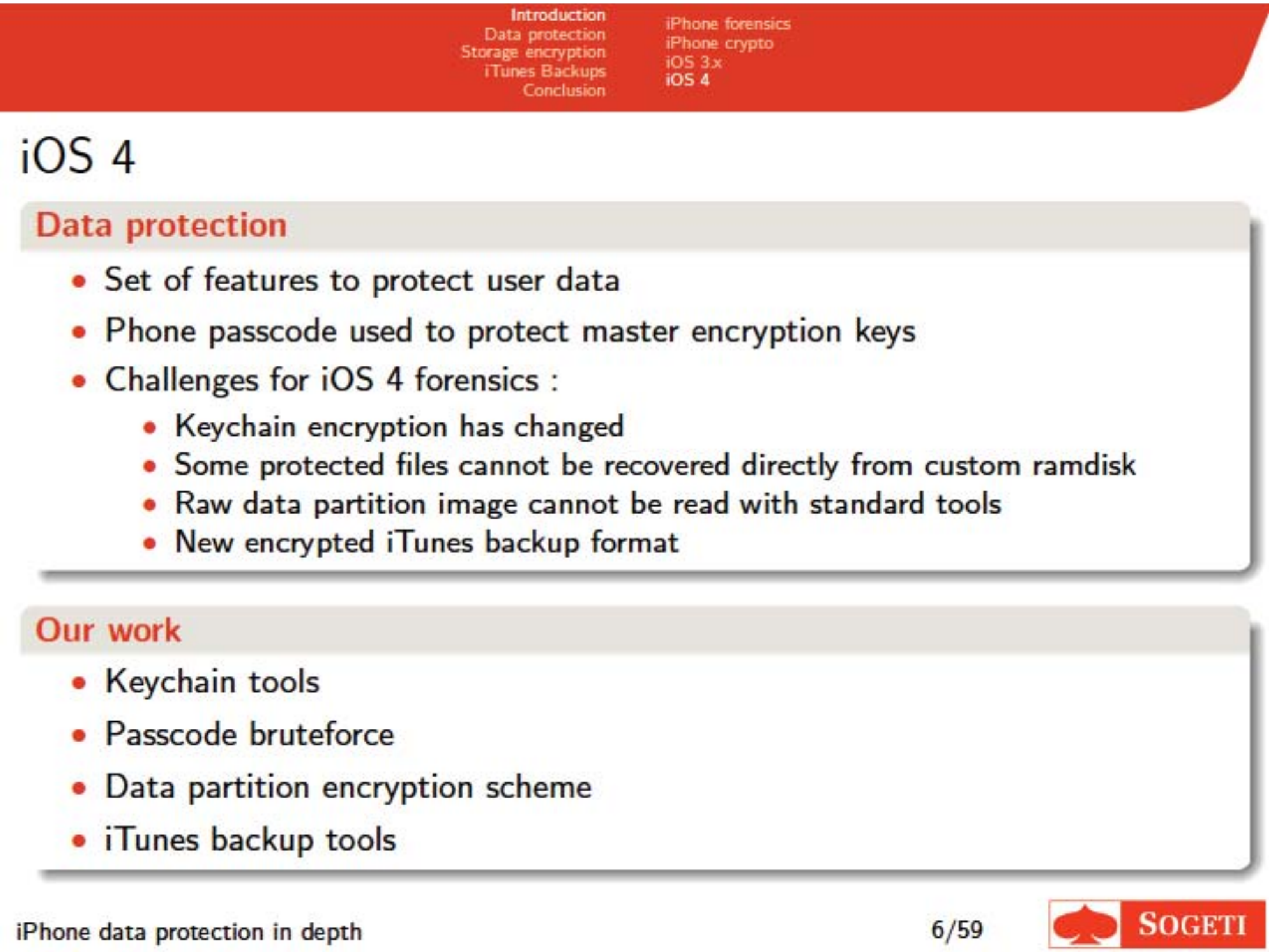
iOS 3.x data protection

Hardware Flash memory encryption

- Introduced with iPhone 3GS
- Allows fast remote wipe
- Data still accessible transparently from custom ramdisk

Keychain

- SQLite database for passwords, certificates and private keys
- Each table has an encrypted data column
- All items encrypted with key 0x835
- Format : IV + AES128(key835, data + SHA1(data), iv)



iOS 4

Data protection

- Set of features to protect user data
- Phone passcode used to protect master encryption keys
- Challenges for iOS 4 forensics :
  - Keychain encryption has changed
  - Some protected files cannot be recovered directly from custom ramdisk
  - Raw data partition image cannot be read with standard tools
  - New encrypted iTunes backup format

Our work

- Keychain tools
- Passcode bruteforce
- Data partition encryption scheme
- iTunes backup tools

Plan

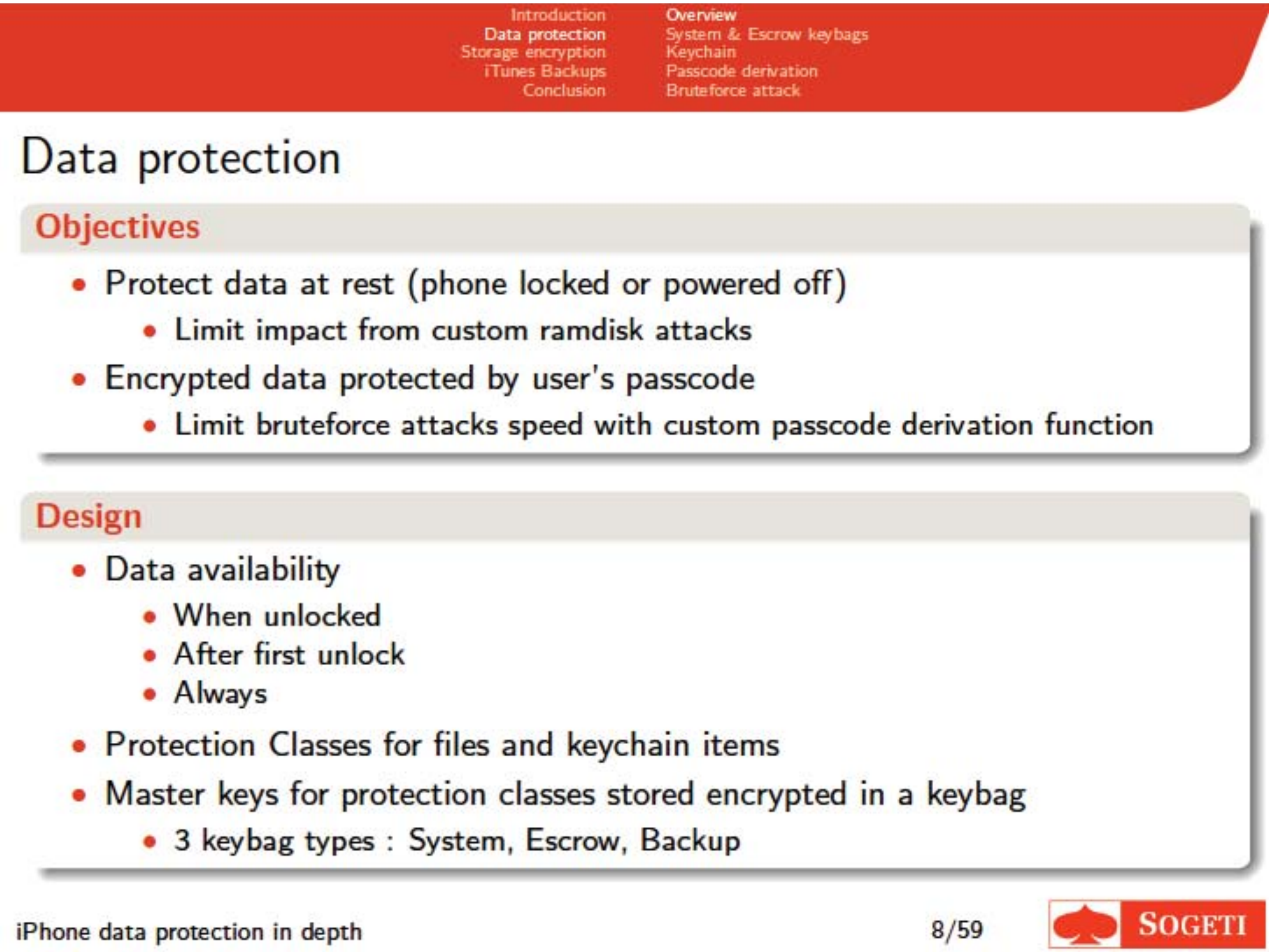
1 Introduction

2 Data protection
- Overview
- System & Escrow keybags
- Keychain
- Passcode derivation
- Bruteforce attack

3 Storage encryption

4 iTunes Backups

5 Conclusion



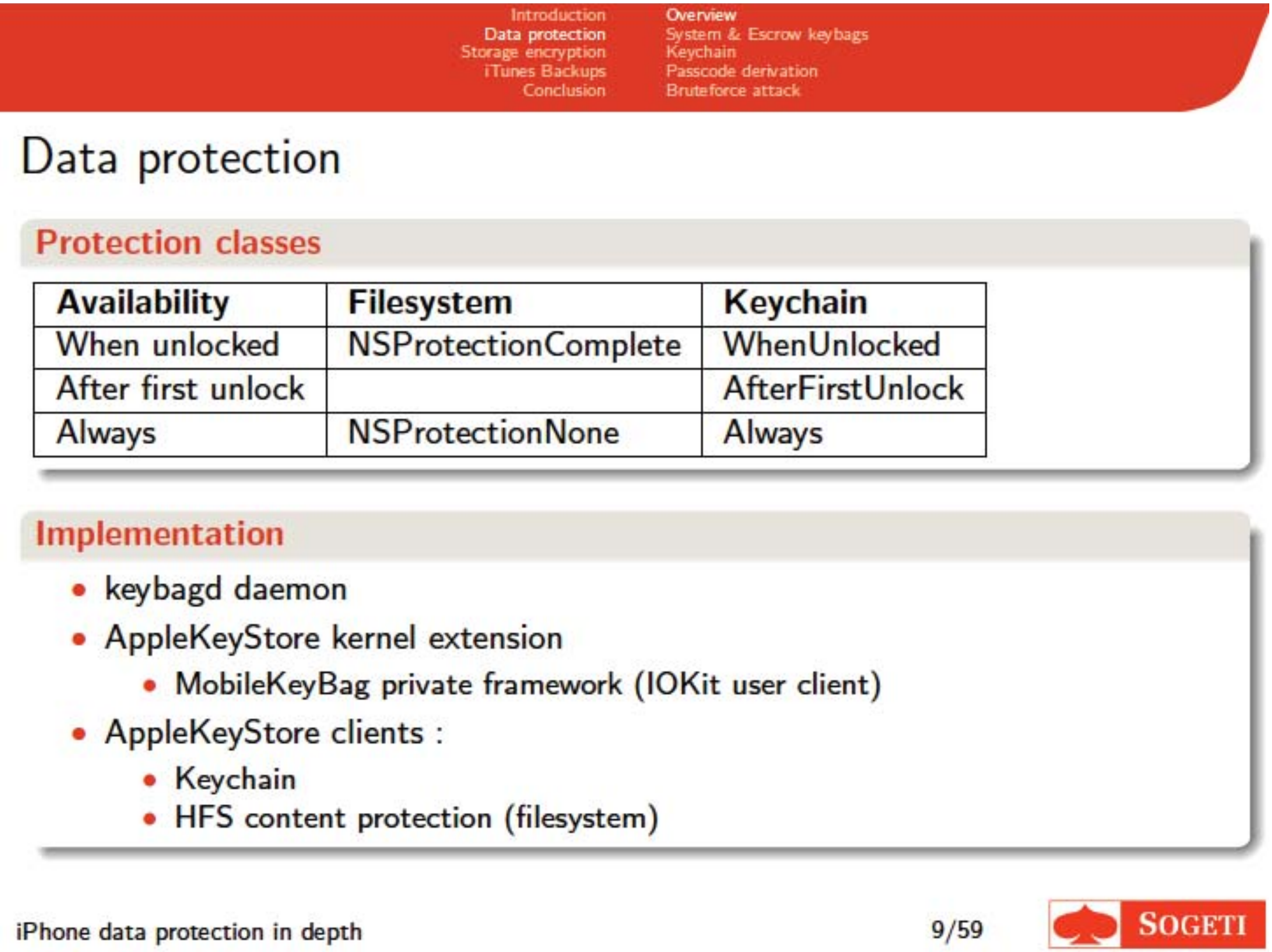
Data protection

Objectives

- Protect data at rest (phone locked or powered off)
  - Limit impact from custom ramdisk attacks
- Encrypted data protected by user's passcode
  - Limit bruteforce attacks speed with custom passcode derivation function

Design

- Data availability
  - When unlocked
  - After first unlock
  - Always
- Protection Classes for files and keychain items
- Master keys for protection classes stored encrypted in a keybag
  - 3 keybag types : System, Escrow, Backup



Data protection

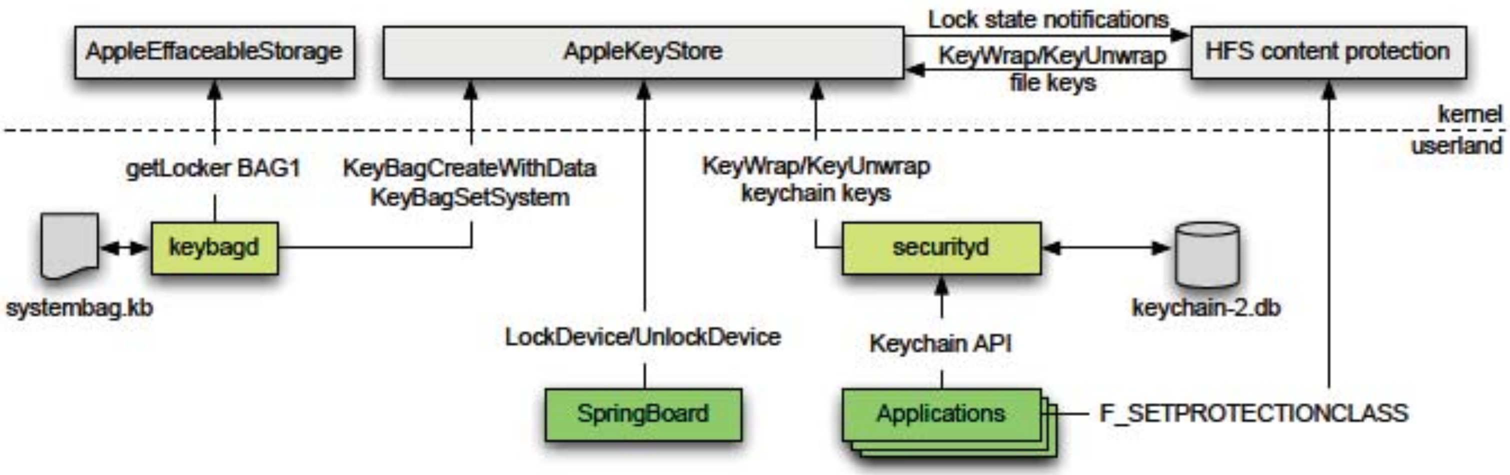
Protection classes

Availability	Filesystem	Keychain
When unlocked	NSProtectionComplete	WhenUnlocked
After first unlock		AfterFirstUnlock
Always	NSProtectionNone	Always

Implementation

- keybagd daemon
- AppleKeyStore kernel extension
  - MobileKeyBag private framework (IOKit user client)
- AppleKeyStore clients :
  - Keychain
  - HFS content protection (filesystem)

Data protection components & interactions



AppleEffaceableStorage

AppleKeyStore

Lock state notifications

KeyWrap/KeyUnwrap
file keys

HFS content protection

kernel

userland

getLocker BAG1

KeyBagCreateWithData
KeyBagSetSystem

KeyWrap/KeyUnwrap
keychain keys

systembag.kb

keybagd

securityd

keychain-2.db

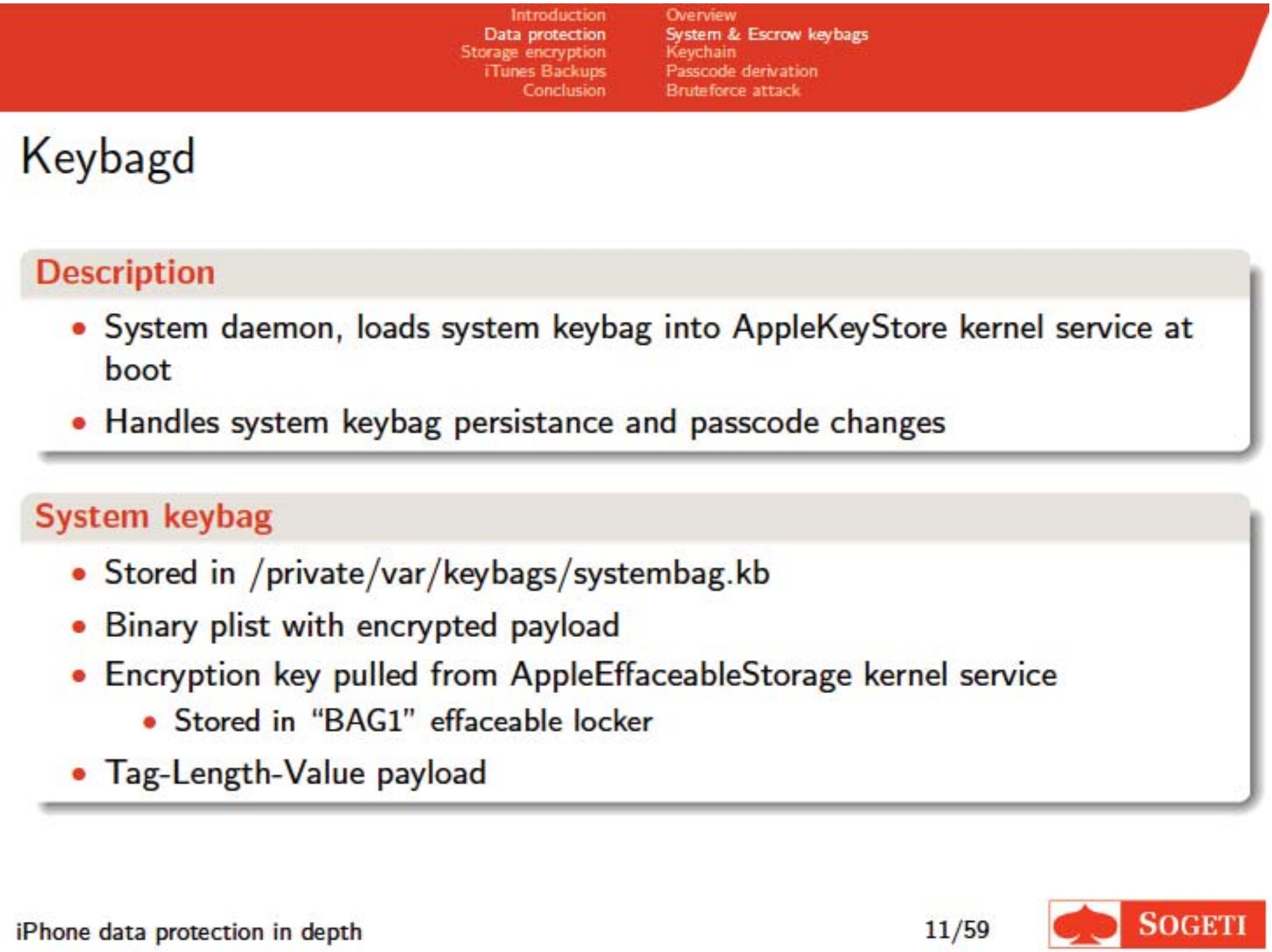
LockDevice/UnlockDevice

Keychain API

SpringBoard

Applications

F_SETPROTECTIONCLASS



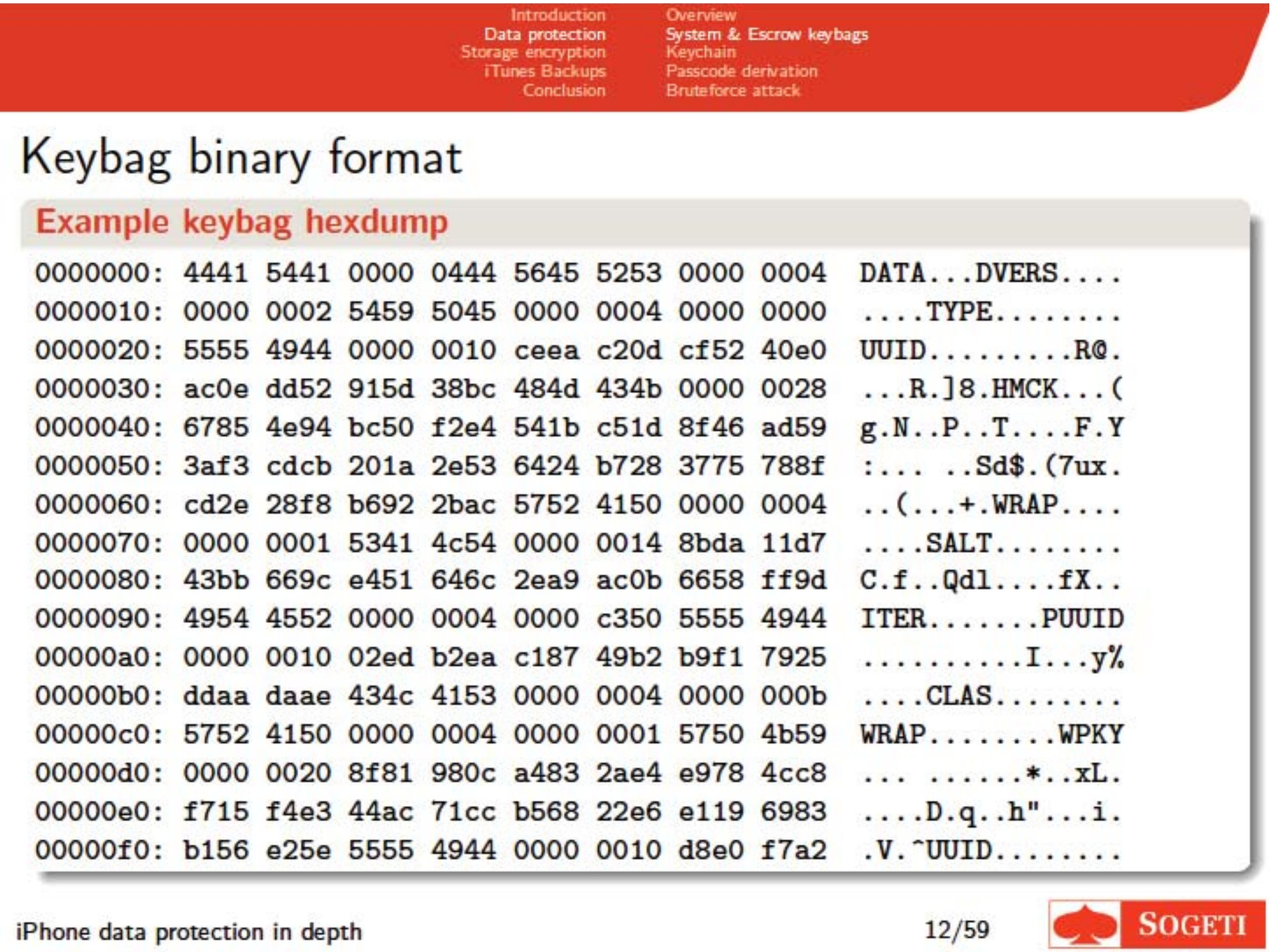
Keybagd

Description

- System daemon, loads system keybag into AppleKeyStore kernel service at boot
- Handles system keybag persistance and passcode changes

System keybag

- Stored in /private/var/keybags/systembag.kb
- Binary plist with encrypted payload
- Encryption key pulled from AppleEffaceableStorage kernel service
  - Stored in "BAG1" effaceable locker
- Tag-Length-Value payload



Introduction
Data protection
Storage encryption
iTunes Backups
Conclusion
Overview
System & Escrow keybags
Keychain
Passcode derivation
Bruteforce attack

Keybag binary format

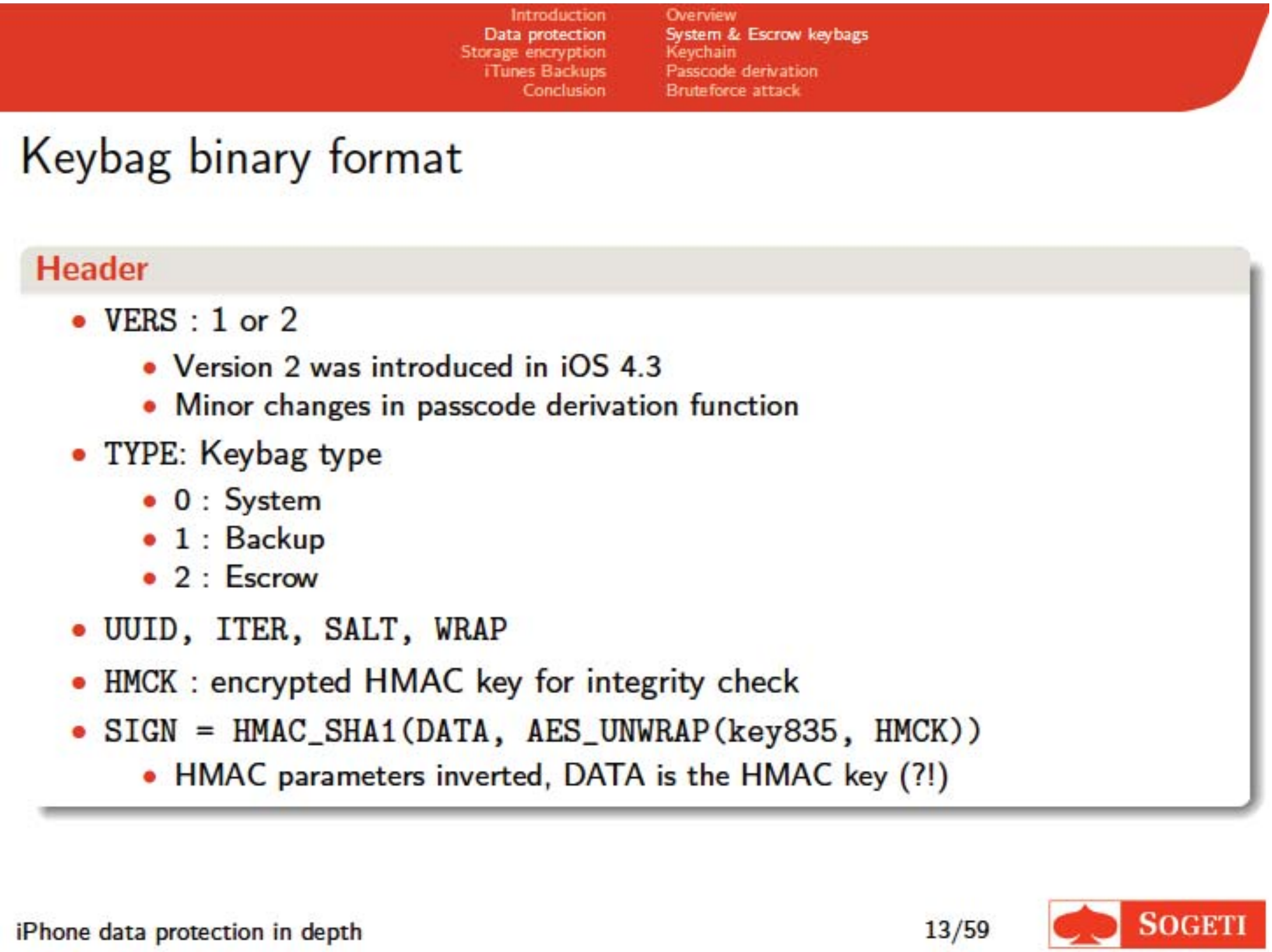
Example keybag hexdump

```
0000000: 4441 5441 0000 0444 5645 5253 0000 0004  DATA...DVERS....
0000010: 0000 0002 5459 5045 0000 0004 0000 0000  ....TYPE........
0000020: 5555 4944 0000 0010 ceea c20d cf52 40e0  UUID.........R@.
0000030: ac0e dd52 915d 38bc 484d 434b 0000 0028  ...R.]8.HMCK...(
0000040: 6785 4e94 bc50 f2e4 541b c51d 8f46 ad59  g.N..P..T....F.Y
0000050: 3af3 cdcb 201a 2e53 6424 b728 3775 788f  :... ..Sd$.(7ux.
0000060: cd2e 28f8 b692 2bac 5752 4150 0000 0004  ..(...+.WRAP....
0000070: 0000 0001 5341 4c54 0000 0014 8bda 11d7  ....SALT........
0000080: 43bb 669c e451 646c 2ea9 ac0b 6658 ff9d  C.f..Qdl....fX..
0000090: 4954 4552 0000 0004 0000 c350 5555 4944  ITER.......PUUID
00000a0: 0000 0010 02ed b2ea c187 49b2 b9f1 7925  ..........I...y%
00000b0: ddaa daae 434c 4153 0000 0004 0000 000b  ....CLAS........
00000c0: 5752 4150 0000 0004 0000 0001 5750 4b59  WRAP........WPKY
00000d0: 0000 0020 8f81 980c a483 2ae4 e978 4cc8  ... ......*..xL.
00000e0: f715 f4e3 44ac 71cc b568 22e6 e119 6983  ....D.q..h"...i.
00000f0: b156 e25e 5555 4944 0000 0010 d8e0 f7a2  .V.^UUID........
```

iPhone data protection in depth

12/59

SOGETI



Keybag binary format

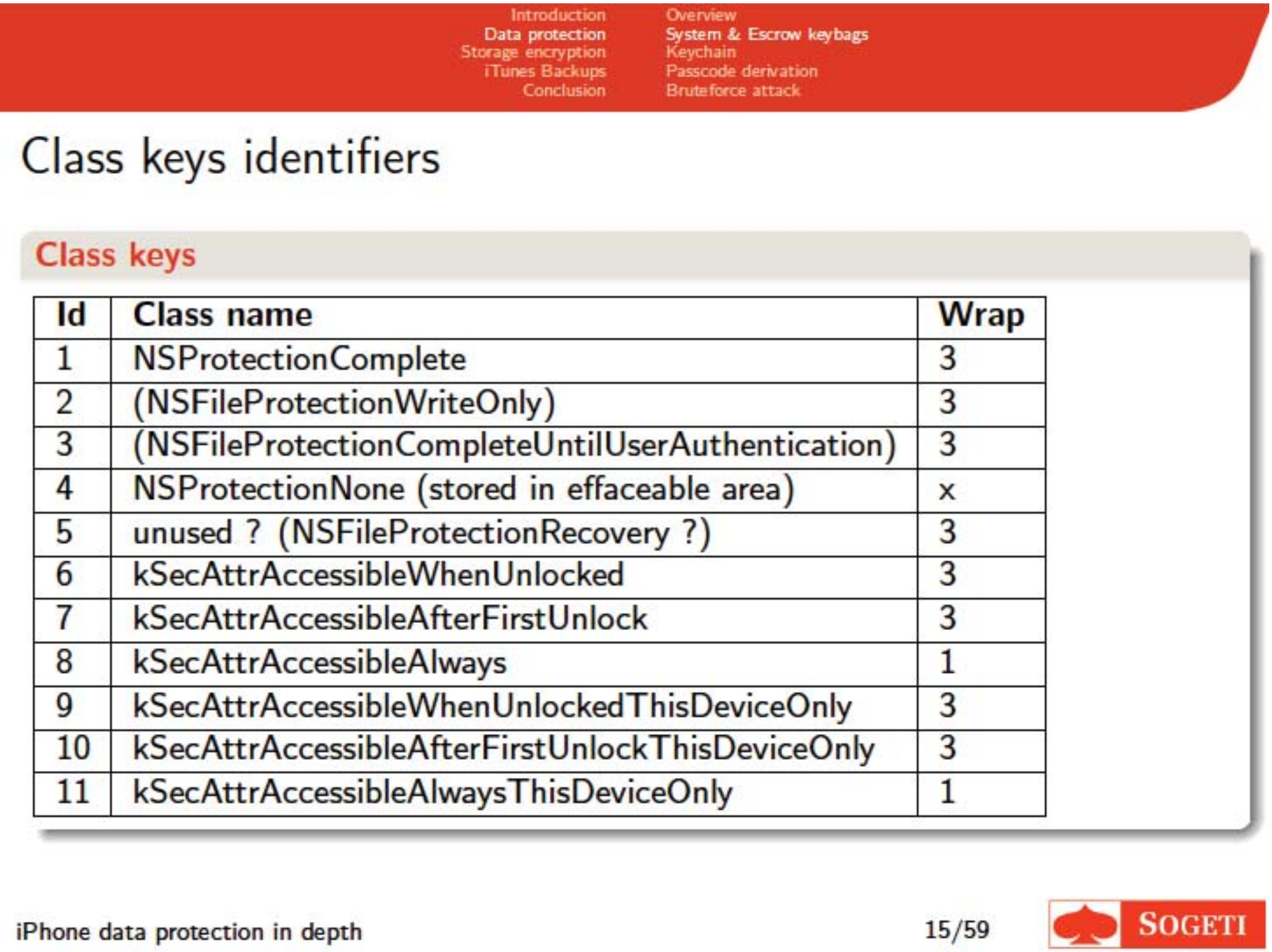
Header

- VERS : 1 or 2
  - Version 2 was introduced in iOS 4.3
  - Minor changes in passcode derivation function
- TYPE: Keybag type
  - 0 : System
  - 1 : Backup
  - 2 : Escrow
- UUID, ITER, SALT, WRAP
- HMCK : encrypted HMAC key for integrity check
- SIGN = HMAC_SHA1(DATA, AES_UNWRAP(key835, HMCK))
  - HMAC parameters inverted, DATA is the HMAC key (?!)

Keybag binary format

Wrapped class keys

- UUID : Key uuid
- CLAS : Class number
- WRAP : Wrap flags
  - 1 : AES encrypted with key 0x835
  - 2 : AES wrapped with passcode key (RFC 3394)
- WPKY : Wrapped key



Introduction
Data protection
Storage encryption
iTunes Backups
Conclusion

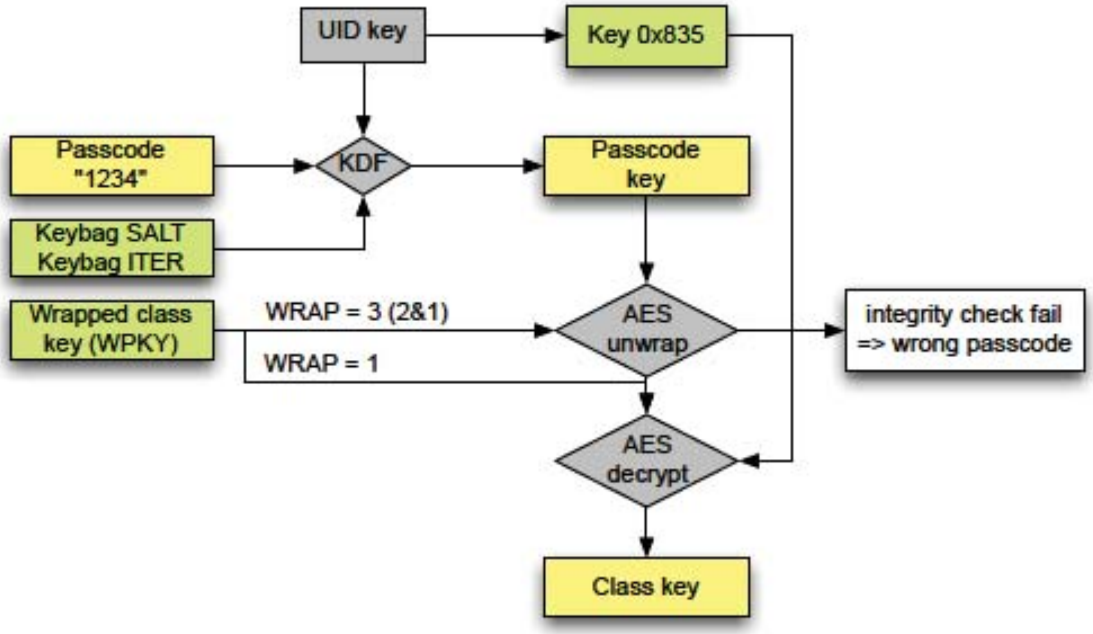
Overview
System & Escrow keybags
Keychain
Passcode derivation
Bruteforce attack

Class keys identifiers

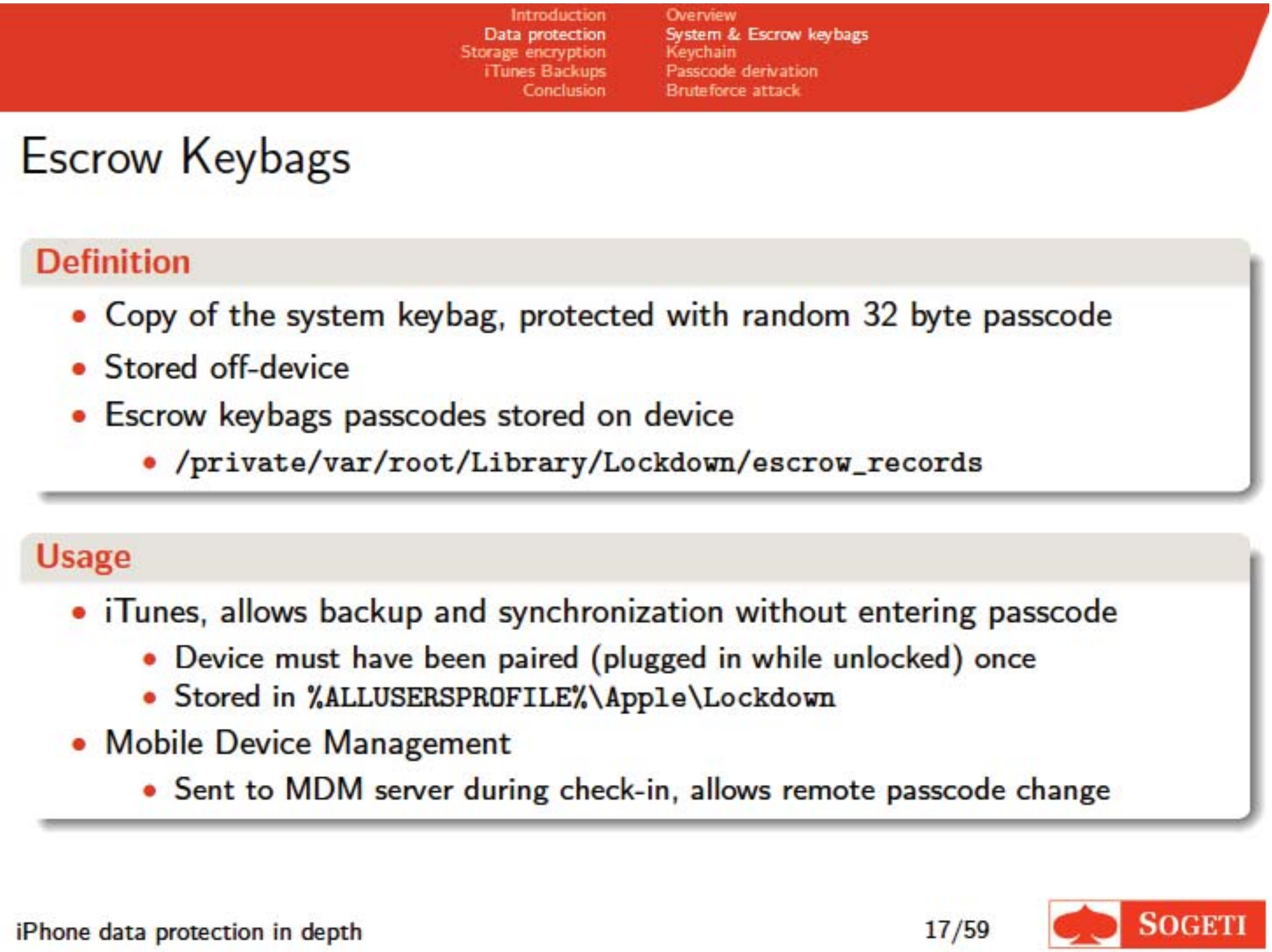
Class keys

Id	Class name	Wrap
1	NSProtectionComplete	3
2	(NSFileProtectionWriteOnly)	3
3	(NSFileProtectionCompleteUntilUserAuthentication)	3
4	NSProtectionNone (stored in effaceable area)	x
5	unused ? (NSFileProtectionRecovery ?)	3
6	kSecAttrAccessibleWhenUnlocked	3
7	kSecAttrAccessibleAfterFirstUnlock	3
8	kSecAttrAccessibleAlways	1
9	kSecAttrAccessibleWhenUnlockedThisDeviceOnly	3
10	kSecAttrAccessibleAfterFirstUnlockThisDeviceOnly	3
11	kSecAttrAccessibleAlwaysThisDeviceOnly	1

Keybag unlock



UID key
Key 0x835
Passcode "1234"
KDF
Passcode key
Keybag SALT
Keybag ITER
Wrapped class key (WPKY)
WRAP = 3 (2&1)
WRAP = 1
AES unwrap
integrity check fail => wrong passcode
AES decrypt
Class key



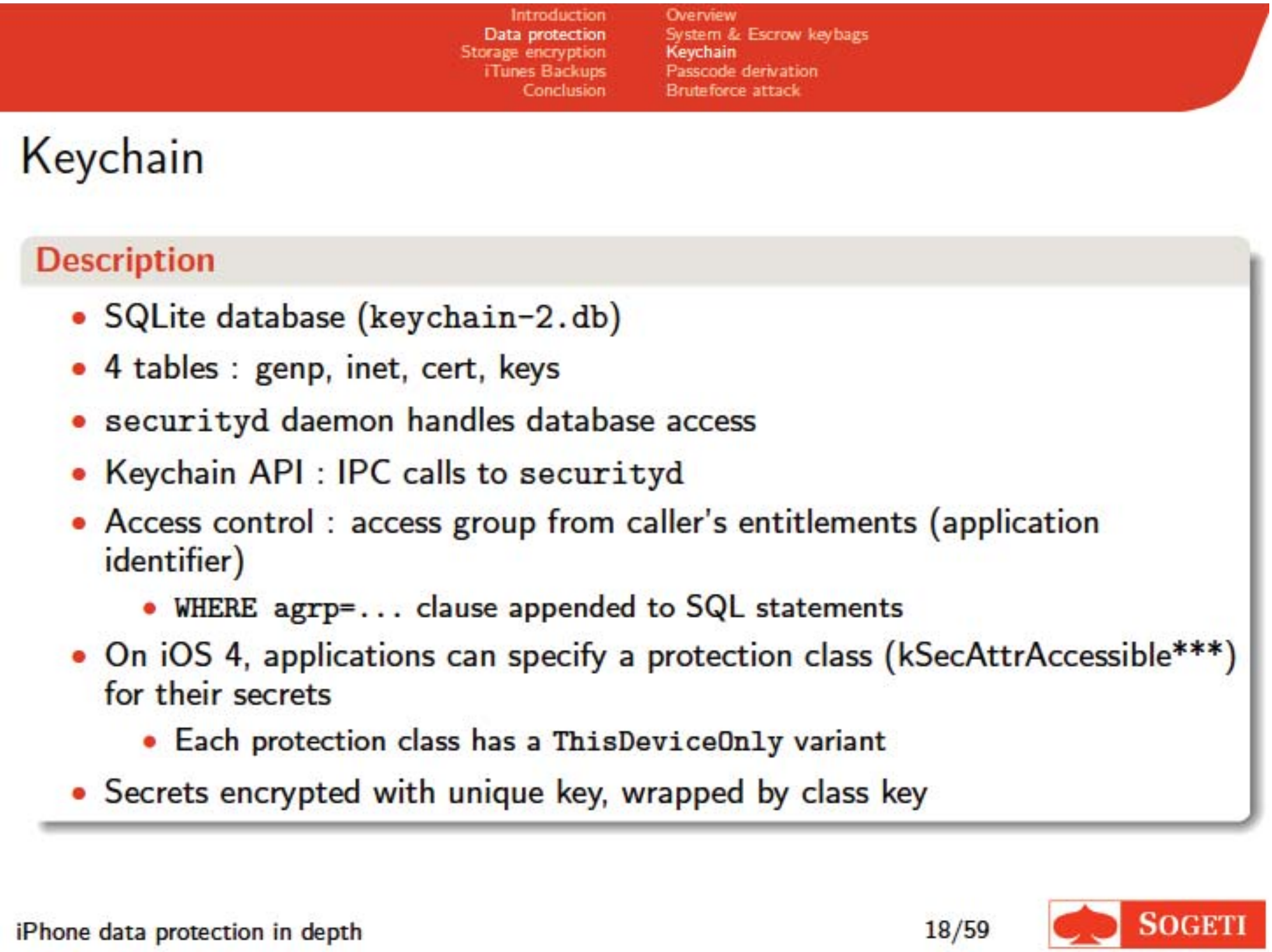
Escrow Keybags

Definition

- Copy of the system keybag, protected with random 32 byte passcode
- Stored off-device
- Escrow keybags passcodes stored on device
  - `/private/var/root/Library/Lockdown/escrow_records`

Usage

- iTunes, allows backup and synchronization without entering passcode
  - Device must have been paired (plugged in while unlocked) once
  - Stored in `%ALLUSERSPROFILE%\Apple\Lockdown`
- Mobile Device Management
  - Sent to MDM server during check-in, allows remote passcode change



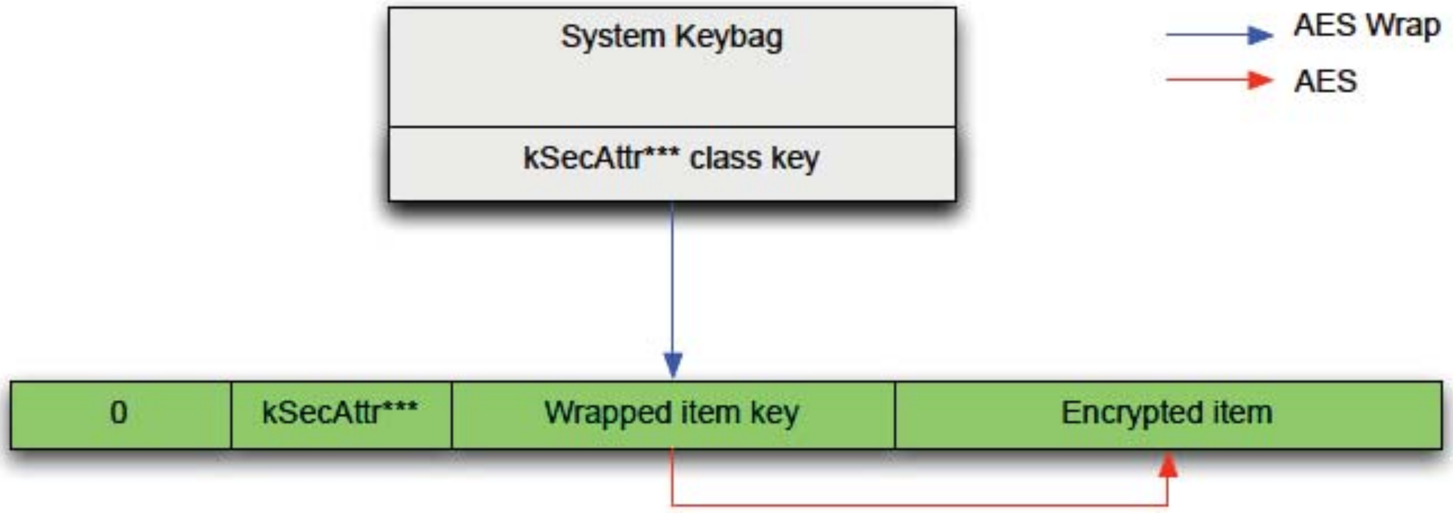
Keychain

Description

- SQLite database (`keychain-2.db`)
- 4 tables : genp, inet, cert, keys
- `securityd` daemon handles database access
- Keychain API : IPC calls to `securityd`
- Access control : access group from caller's entitlements (application identifier)
  - `WHERE agrp=...` clause appended to SQL statements
- On iOS 4, applications can specify a protection class (kSecAttrAccessible***) for their secrets
  - Each protection class has a `ThisDeviceOnly` variant
- Secrets encrypted with unique key, wrapped by class key

Keychain

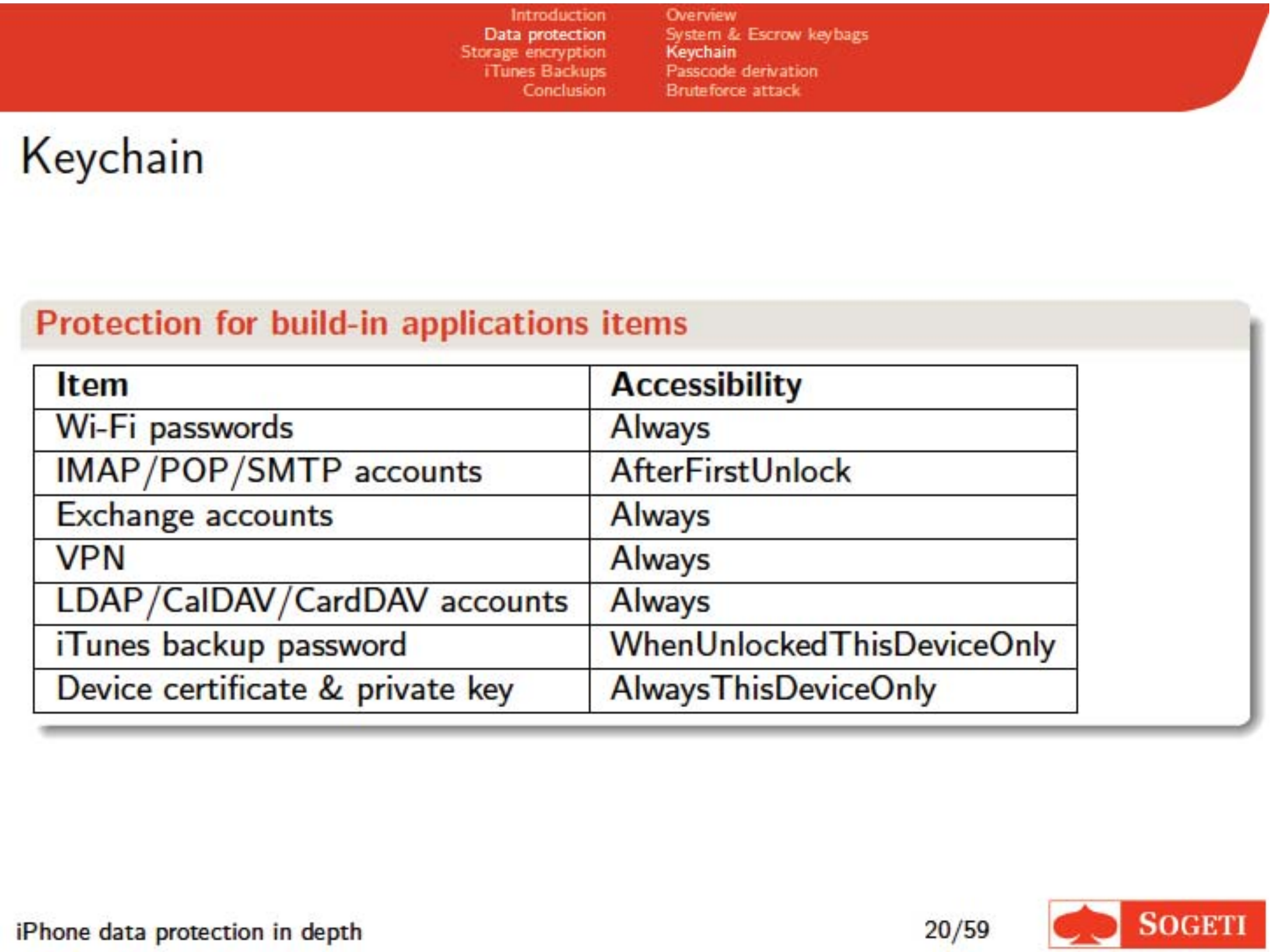
Data column format



System Keybag

kSecAttr*** class key

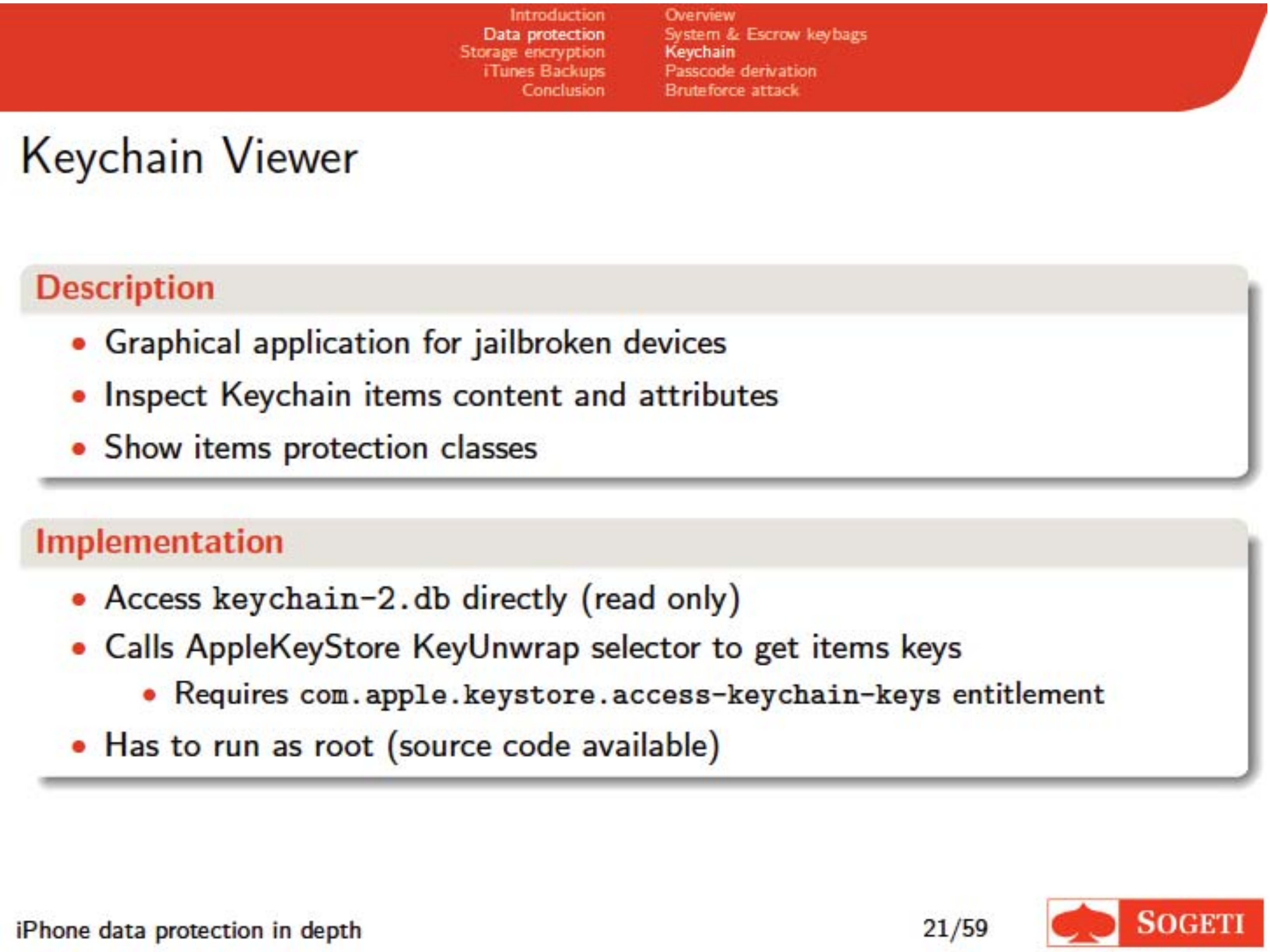
0	kSecAttr***	Wrapped item key	Encrypted item



Keychain

Protection for build-in applications items

Item	Accessibility
Wi-Fi passwords	Always
IMAP/POP/SMTP accounts	AfterFirstUnlock
Exchange accounts	Always
VPN	Always
LDAP/CalDAV/CardDAV accounts	Always
iTunes backup password	WhenUnlockedThisDeviceOnly
Device certificate & private key	AlwaysThisDeviceOnly



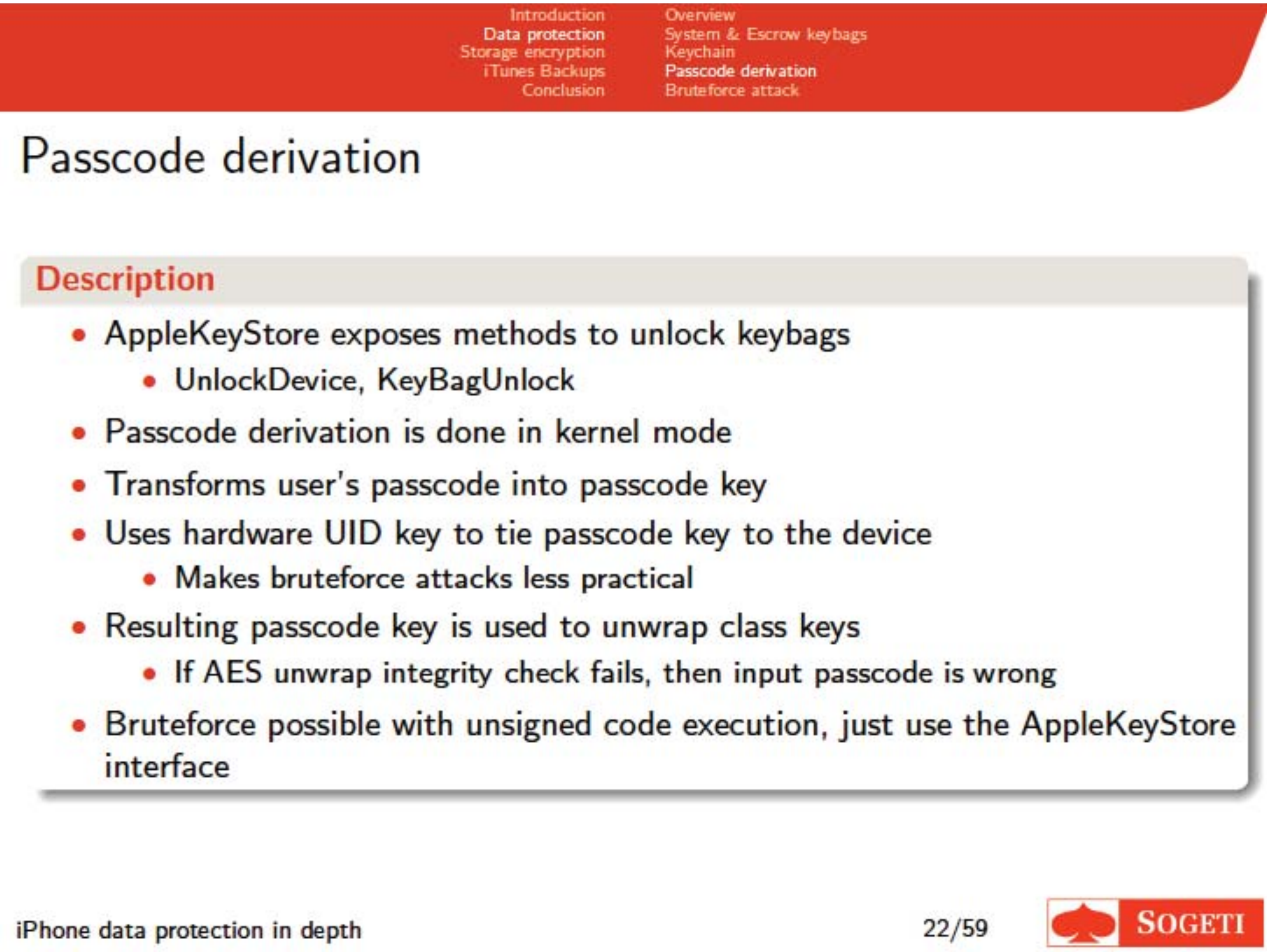
Keychain Viewer

Description

- Graphical application for jailbroken devices
- Inspect Keychain items content and attributes
- Show items protection classes

Implementation

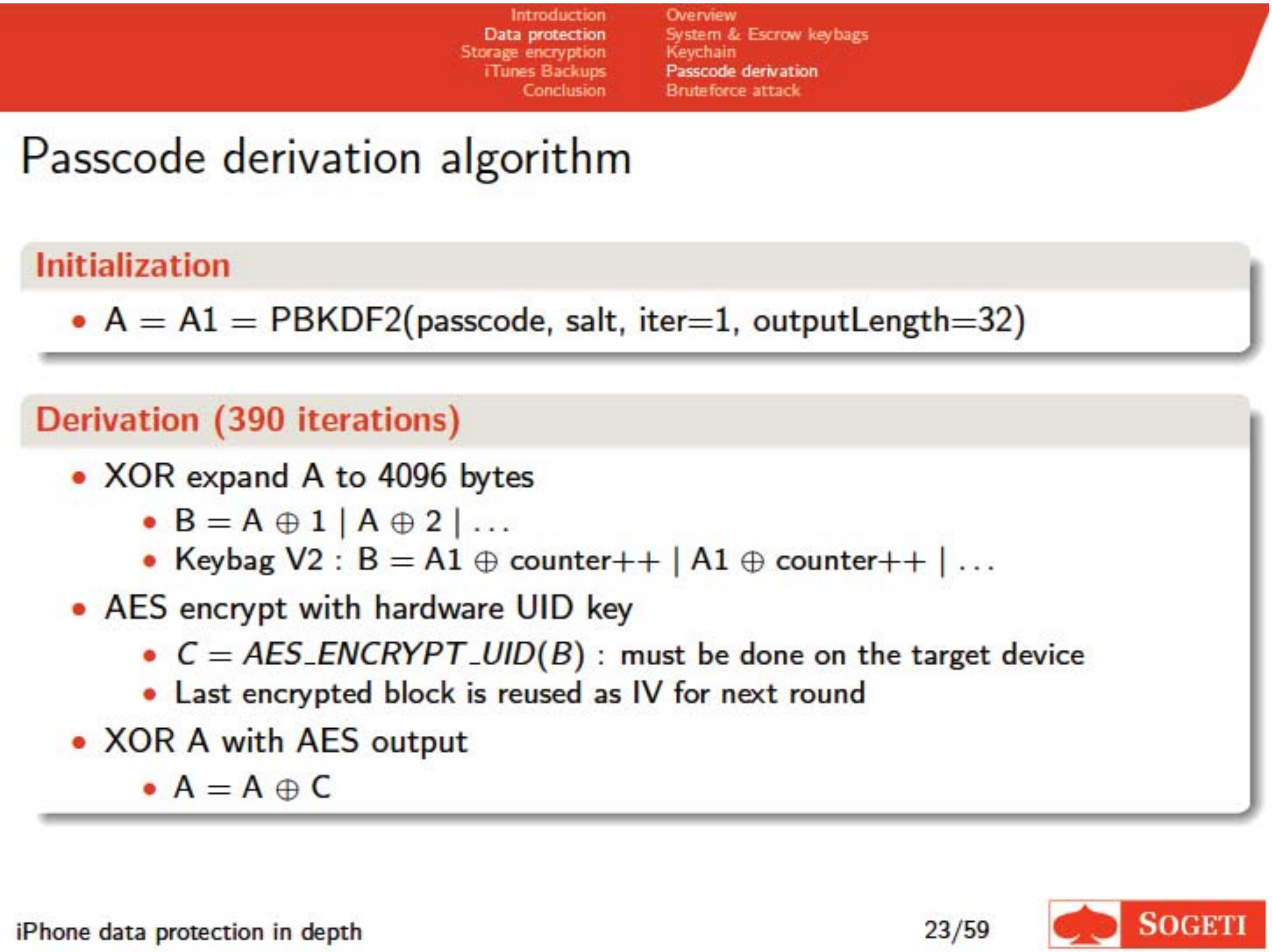
- Access `keychain-2.db` directly (read only)
- Calls AppleKeyStore KeyUnwrap selector to get items keys
    - Requires `com.apple.keystore.access-keychain-keys` entitlement
- Has to run as root (source code available)



Passcode derivation

Description

- AppleKeyStore exposes methods to unlock keybags
  - UnlockDevice, KeyBagUnlock
- Passcode derivation is done in kernel mode
- Transforms user's passcode into passcode key
- Uses hardware UID key to tie passcode key to the device
  - Makes bruteforce attacks less practical
- Resulting passcode key is used to unwrap class keys
  - If AES unwrap integrity check fails, then input passcode is wrong
- Bruteforce possible with unsigned code execution, just use the AppleKeyStore interface



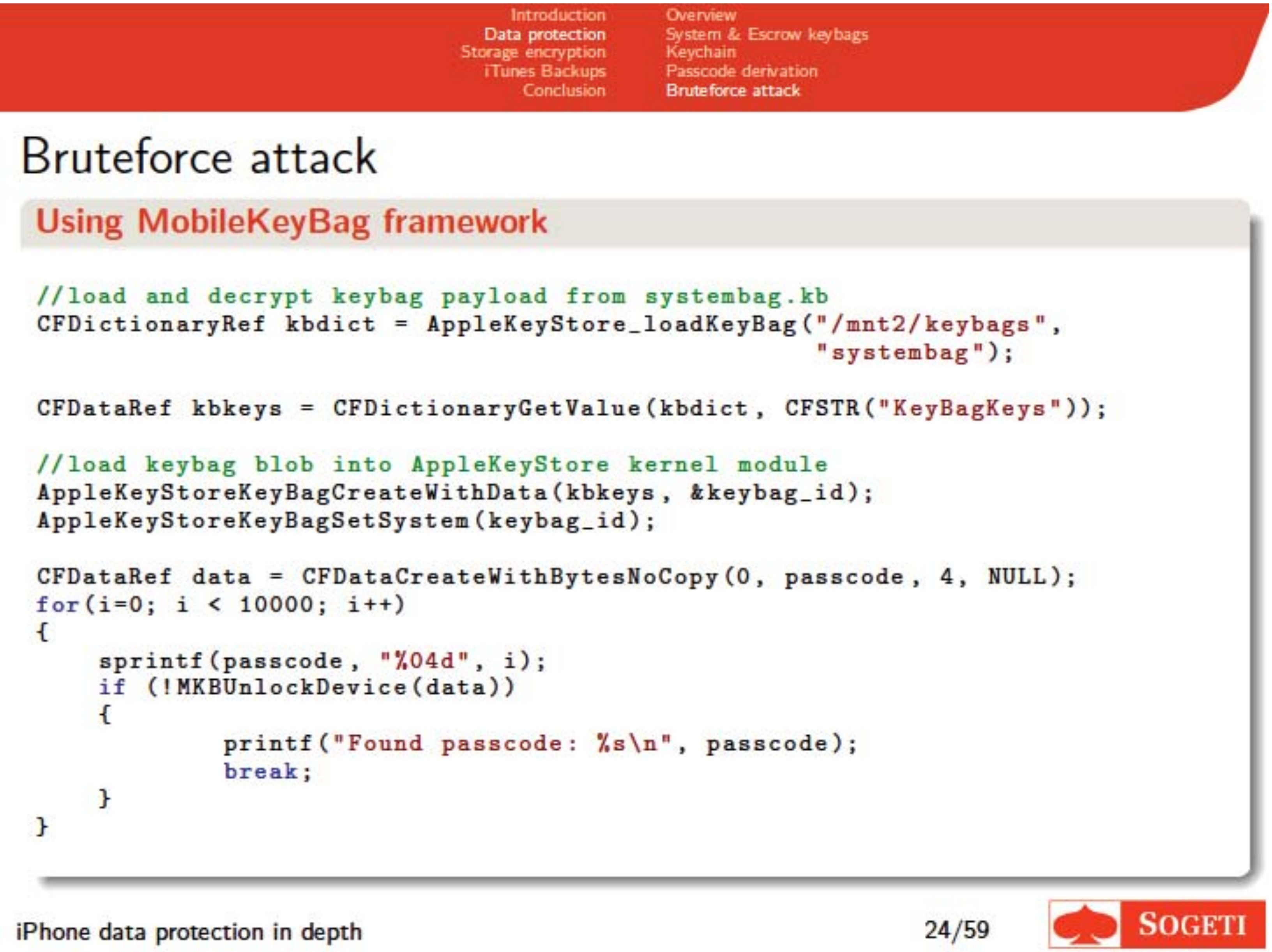
Passcode derivation algorithm

Initialization

- A = A1 = PBKDF2(passcode, salt, iter=1, outputLength=32)

Derivation (390 iterations)

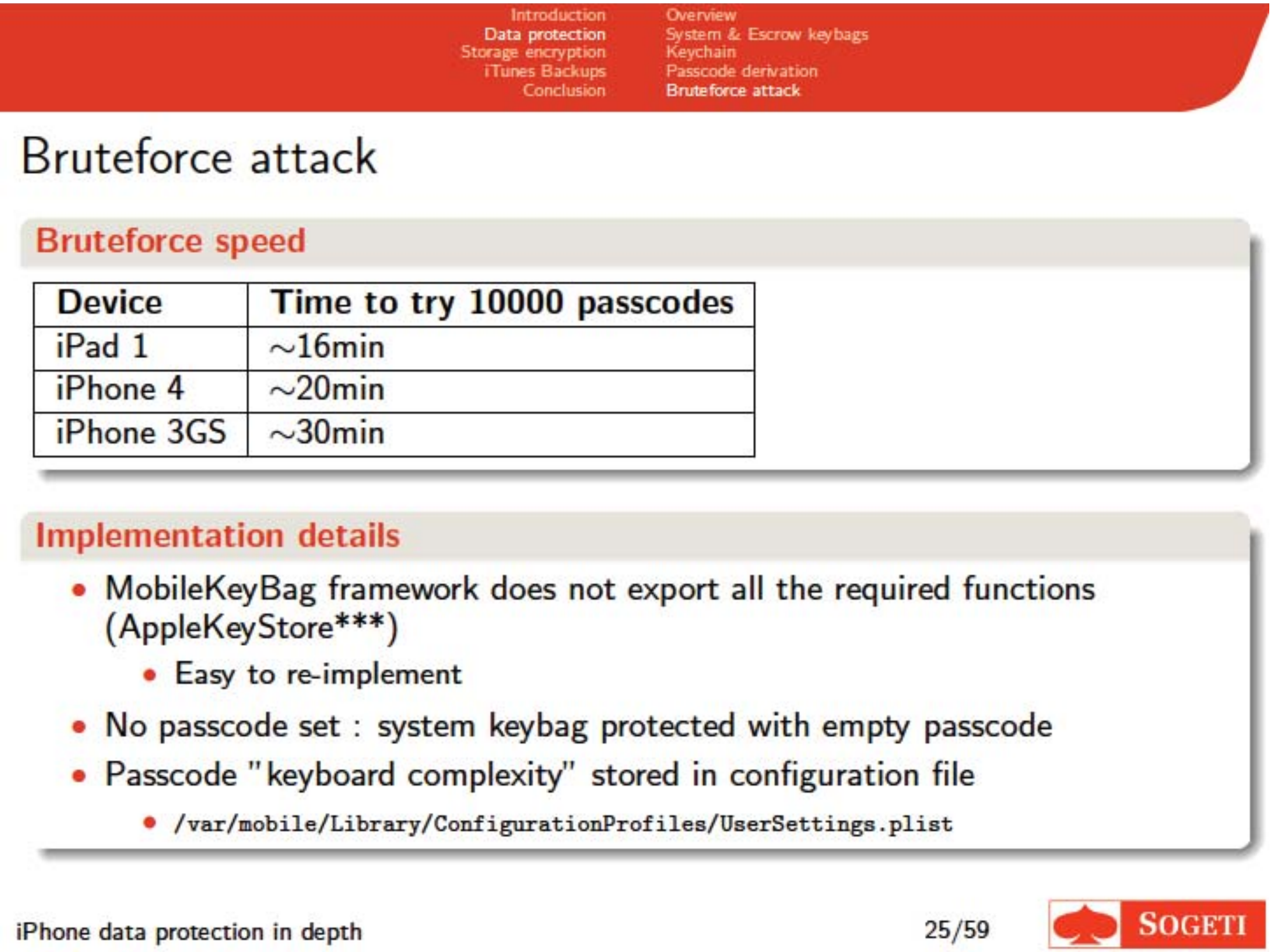
- XOR expand A to 4096 bytes
  - $B = A \oplus 1 \mid A \oplus 2 \mid \ldots$
  - Keybag V2 : $B = A1 \oplus counter{+}{+} \mid A1 \oplus counter{+}{+} \mid \ldots$
- AES encrypt with hardware UID key
  - $C = AES\_ENCRYPT\_UID(B)$: must be done on the target device
  - Last encrypted block is reused as IV for next round
- XOR A with AES output
  - $A = A \oplus C$



Bruteforce attack

Using MobileKeyBag framework

```
//load and decrypt keybag payload from systembag.kb
CFDictionaryRef kbdict = AppleKeyStore_loadKeyBag("/mnt2/keybags",
                                                  "systembag");

CFDataRef kbkeys = CFDictionaryGetValue(kbdict, CFSTR("KeyBagKeys"));

//load keybag blob into AppleKeyStore kernel module
AppleKeyStoreKeyBagCreateWithData(kbkeys, &keybag_id);
AppleKeyStoreKeyBagSetSystem(keybag_id);

CFDataRef data = CFDataCreateWithBytesNoCopy(0, passcode, 4, NULL);
for(i=0; i < 10000; i++)
{
    sprintf(passcode, "%04d", i);
    if (!MKBUnlockDevice(data))
    {
            printf("Found passcode: %s\n", passcode);
            break;
    }
}
```



Bruteforce attack

Bruteforce speed

Device	Time to try 10000 passcodes
iPad 1	~16min
iPhone 4	~20min
iPhone 3GS	~30min

Implementation details

- MobileKeyBag framework does not export all the required functions (AppleKeyStore***)
  - Easy to re-implement
- No passcode set : system keybag protected with empty passcode
- Passcode "keyboard complexity" stored in configuration file
  - `/var/mobile/Library/ConfigurationProfiles/UserSettings.plist`

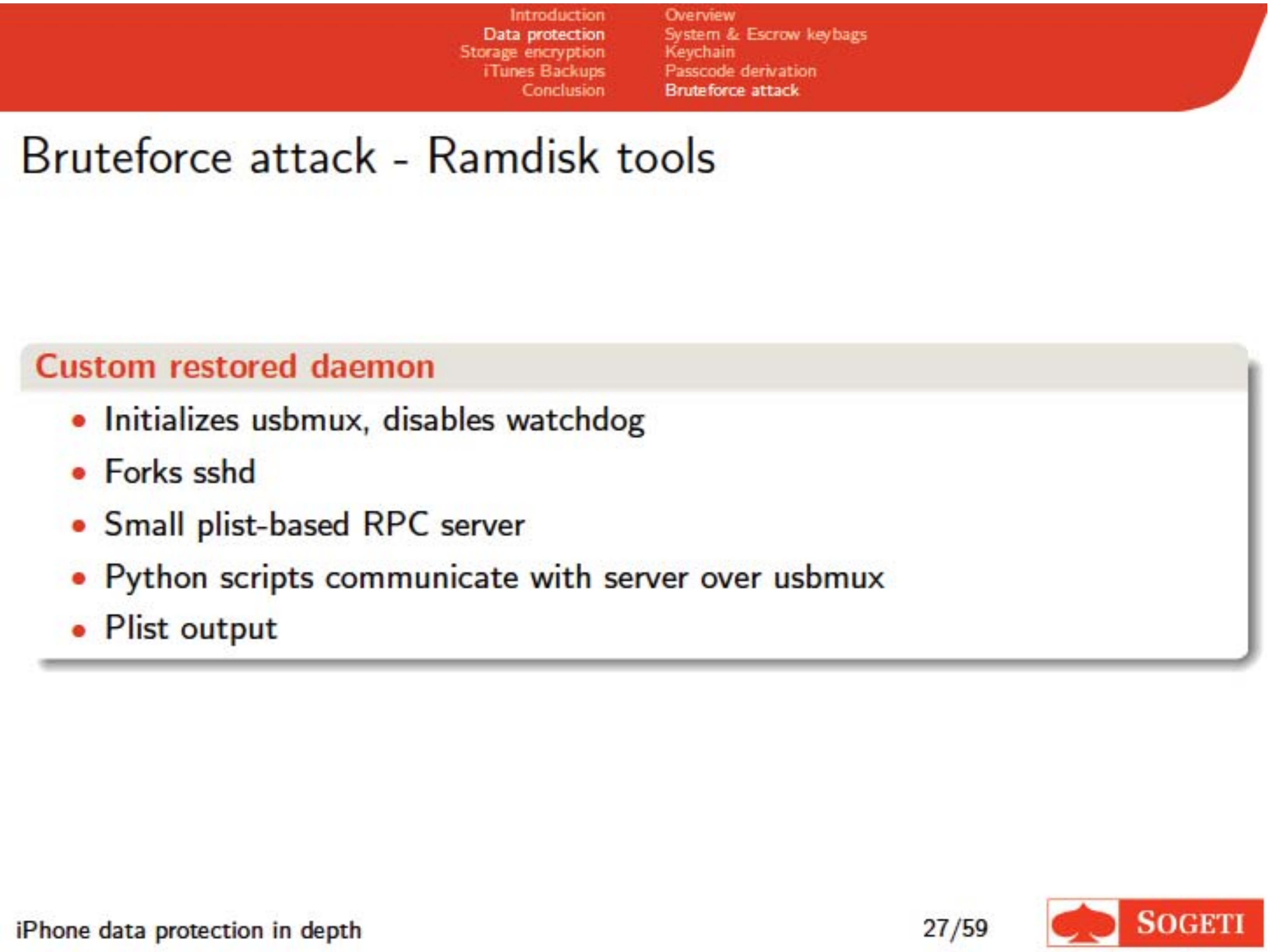
Bruteforce attack - Custom ramdisk

Ramdisk creation

- Extract restore ramdisk from any 4.x ipsw
- Add msft_guy sshd package (ssh.tar)
- Add bruteforce/key extractor tools

Ramdisk bootstrap

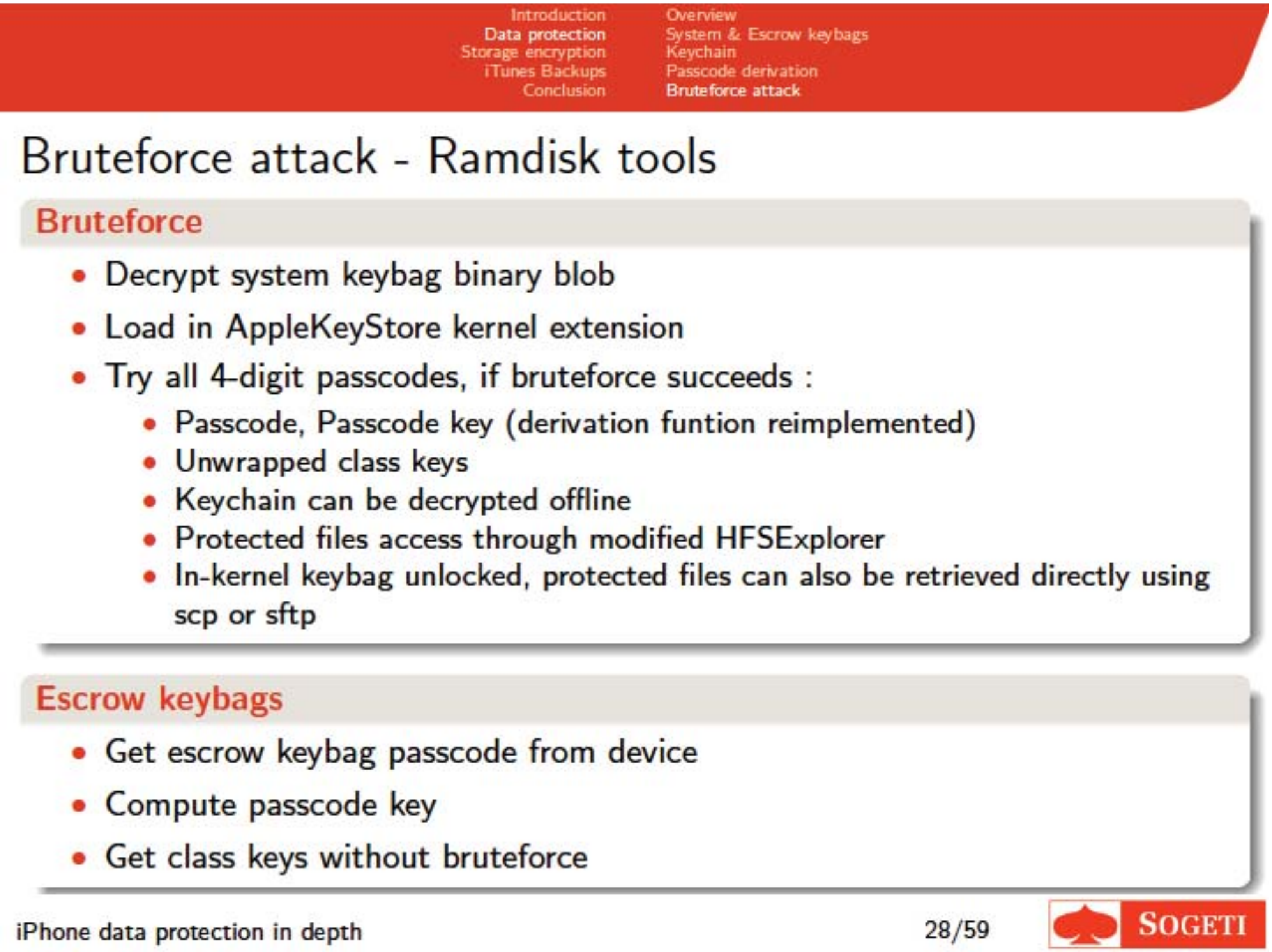
- Chronic dev team syringe injection tool (DFU mode exploits)
- Minimal cyanide payload patches kernel before booting
  - Patch IOAESAccelerator kext to allow UID key usage
  - Once passcode is found we can compute the passcode key from userland
- Same payload and ramdisk works on all A4 devices and iPhone 3GS



Bruteforce attack - Ramdisk tools

Custom restored daemon

- Initializes usbmux, disables watchdog
- Forks sshd
- Small plist-based RPC server
- Python scripts communicate with server over usbmux
- Plist output



Bruteforce attack - Ramdisk tools

Bruteforce

- Decrypt system keybag binary blob
- Load in AppleKeyStore kernel extension
- Try all 4-digit passcodes, if bruteforce succeeds :
  - Passcode, Passcode key (derivation funtion reimplemented)
  - Unwrapped class keys
  - Keychain can be decrypted offline
  - Protected files access through modified HFSExplorer
  - In-kernel keybag unlocked, protected files can also be retrieved directly using scp or sftp

Escrow keybags

- Get escrow keybag passcode from device
- Compute passcode key
- Get class keys without bruteforce

Plan

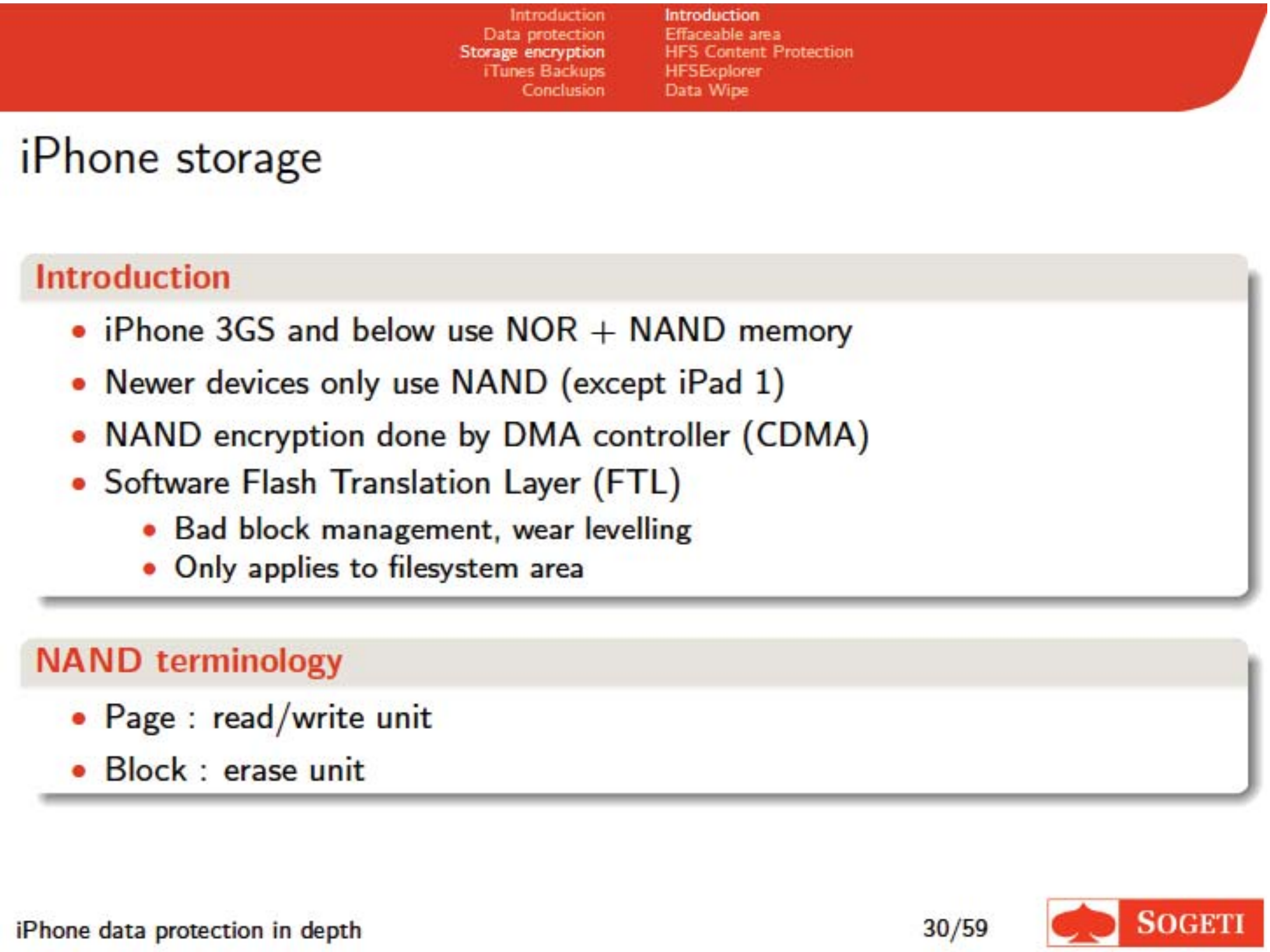
1 Introduction

2 Data protection

3 Storage encryption
- Introduction
- Effaceable area
- HFS Content Protection
- HFSExplorer
- Data Wipe

4 iTunes Backups

5 Conclusion



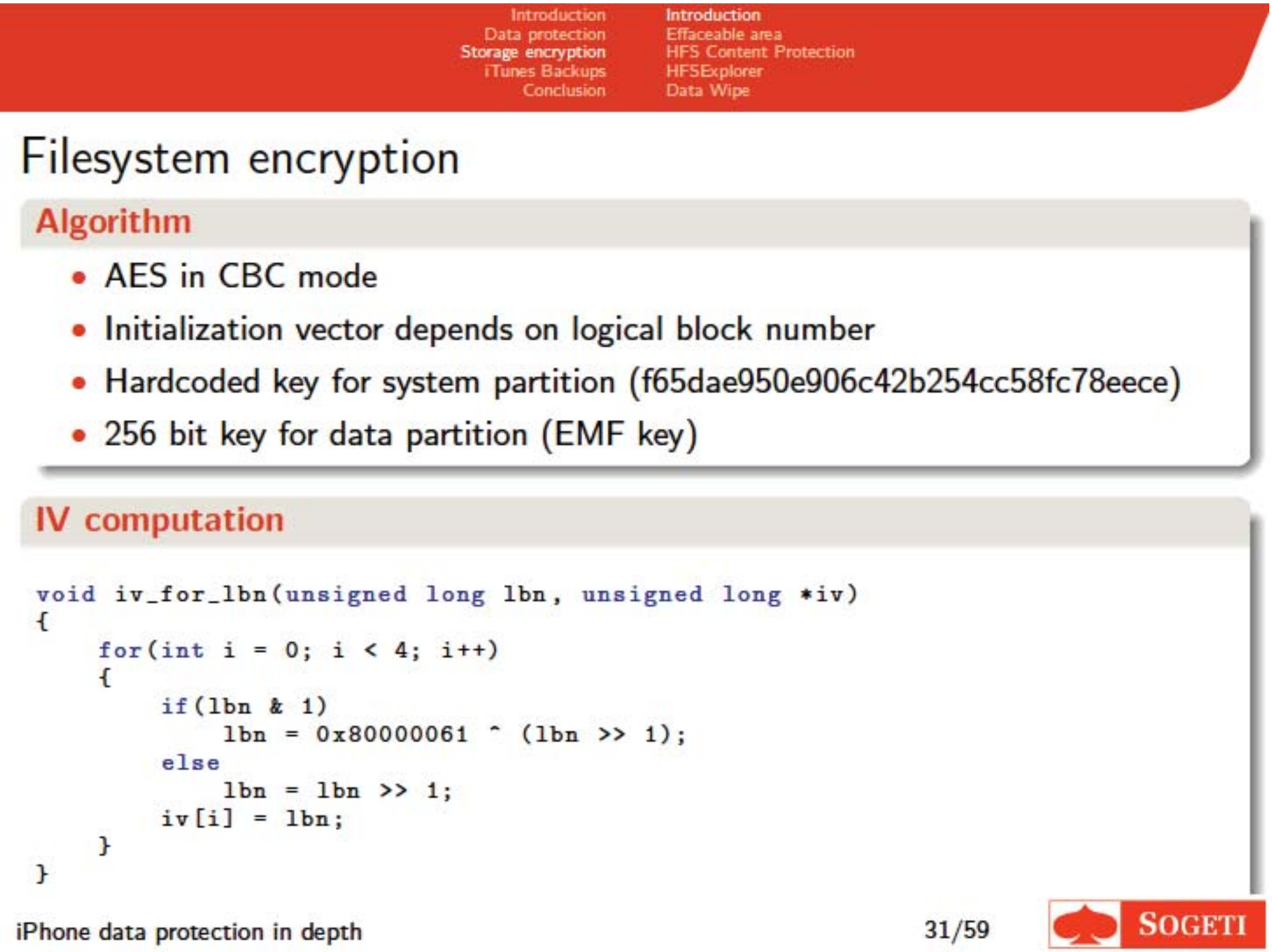
iPhone storage

Introduction

- iPhone 3GS and below use NOR + NAND memory
- Newer devices only use NAND (except iPad 1)
- NAND encryption done by DMA controller (CDMA)
- Software Flash Translation Layer (FTL)
  - Bad block management, wear levelling
  - Only applies to filesystem area

NAND terminology

- Page : read/write unit
- Block : erase unit



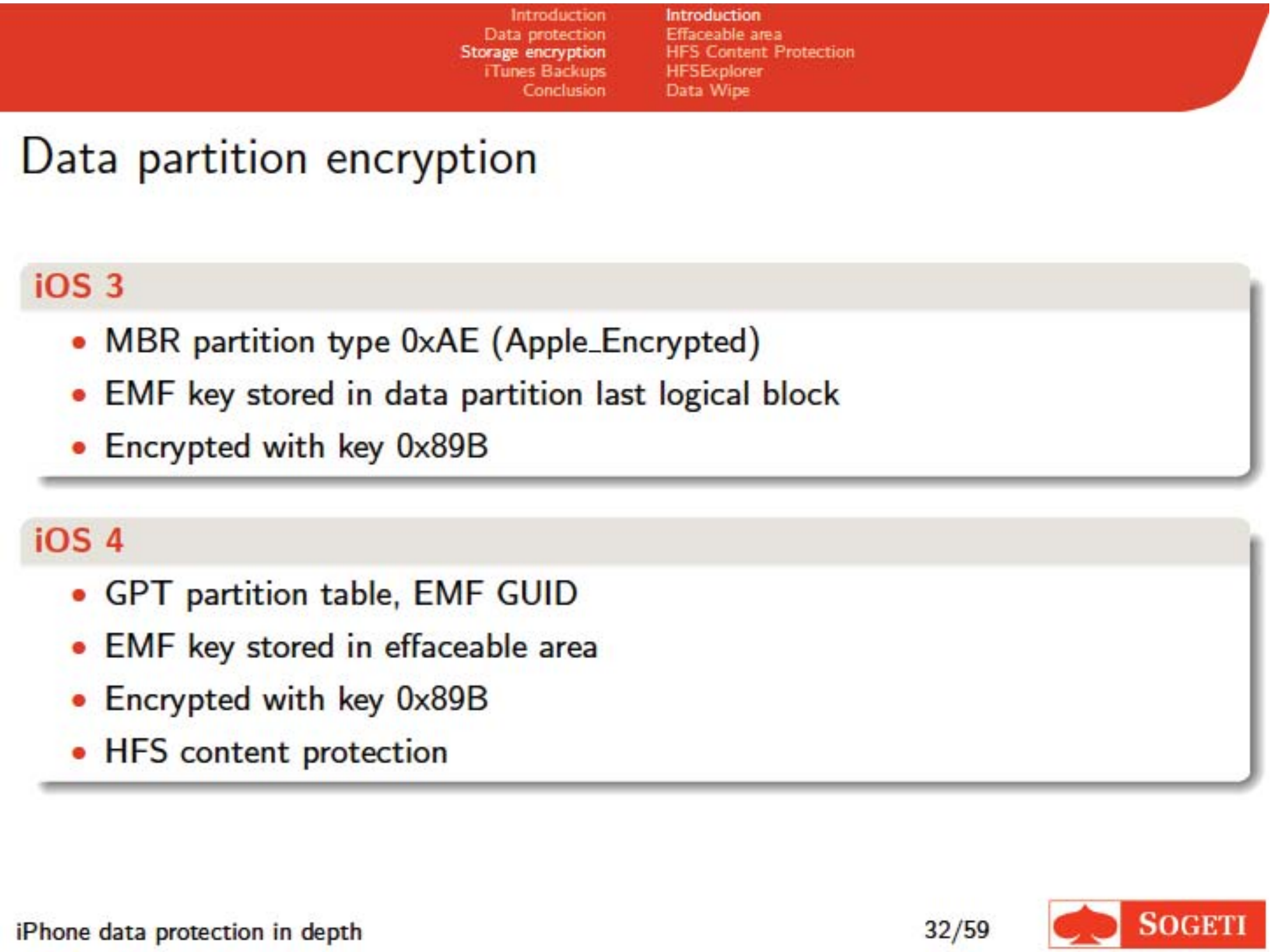
Filesystem encryption

Algorithm

- AES in CBC mode
- Initialization vector depends on logical block number
- Hardcoded key for system partition (f65dae950e906c42b254cc58fc78eece)
- 256 bit key for data partition (EMF key)

IV computation

```
void iv_for_lbn(unsigned long lbn, unsigned long *iv)
{
    for(int i = 0; i < 4; i++)
    {
        if(lbn & 1)
            lbn = 0x80000061 ^ (lbn >> 1);
        else
            lbn = lbn >> 1;
        iv[i] = lbn;
    }
}
```



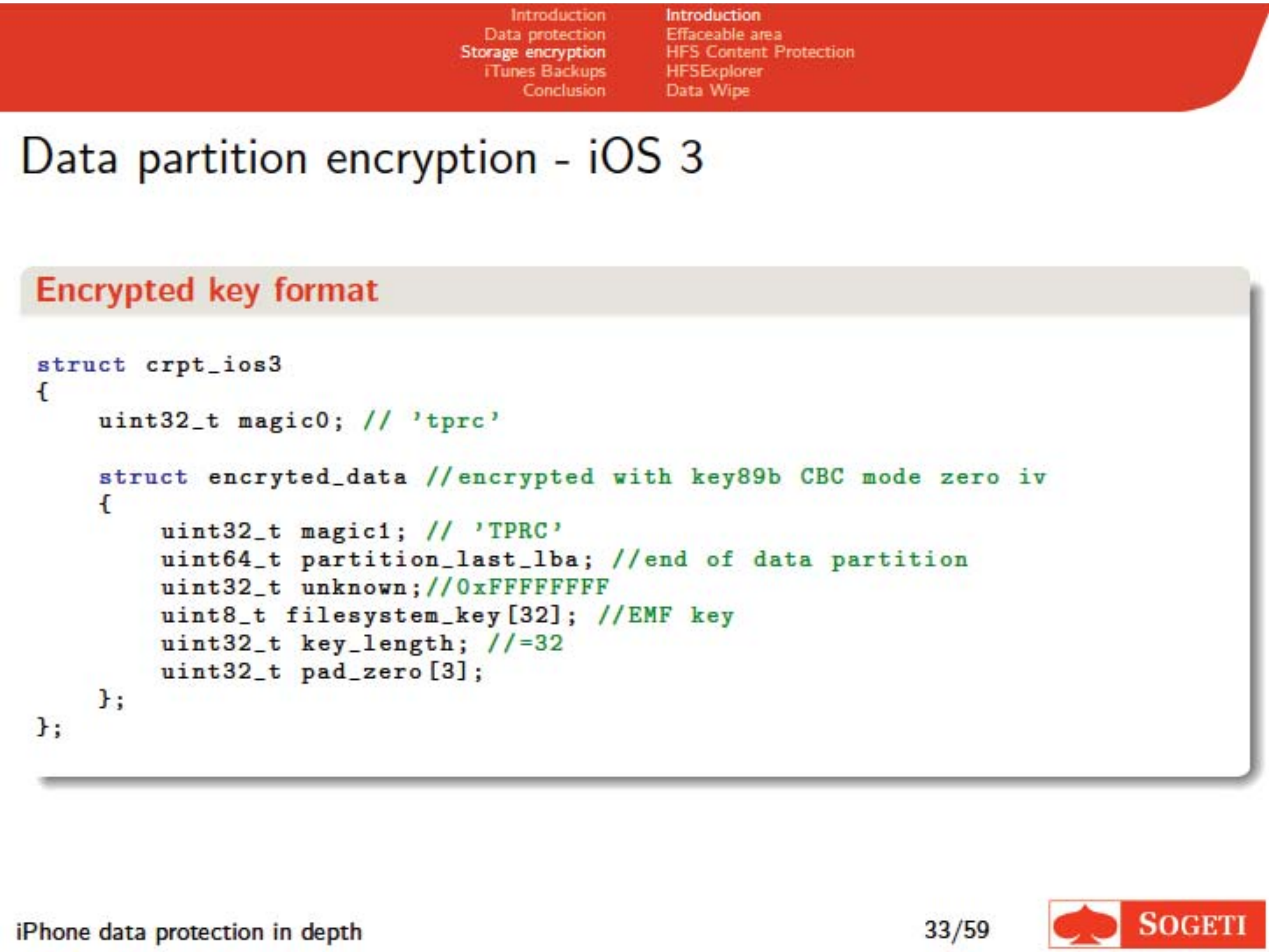
Data partition encryption

iOS 3

- MBR partition type 0xAE (Apple_Encrypted)
- EMF key stored in data partition last logical block
- Encrypted with key 0x89B

iOS 4

- GPT partition table, EMF GUID
- EMF key stored in effaceable area
- Encrypted with key 0x89B
- HFS content protection



Data partition encryption - iOS 3

Encrypted key format

```
struct crpt_ios3
{
    uint32_t magic0; // ’tprc’

    struct encryted_data //encrypted with key89b CBC mode zero iv
    {
        uint32_t magic1; // ’TPRC’
        uint64_t partition_last_lba; //end of data partition
        uint32_t unknown;//0xFFFFFFFF
        uint8_t filesystem_key[32]; //EMF key
        uint32_t key_length; //=32
        uint32_t pad_zero[3];
    };
};
```

iOS 4 NAND layout

Container partitions

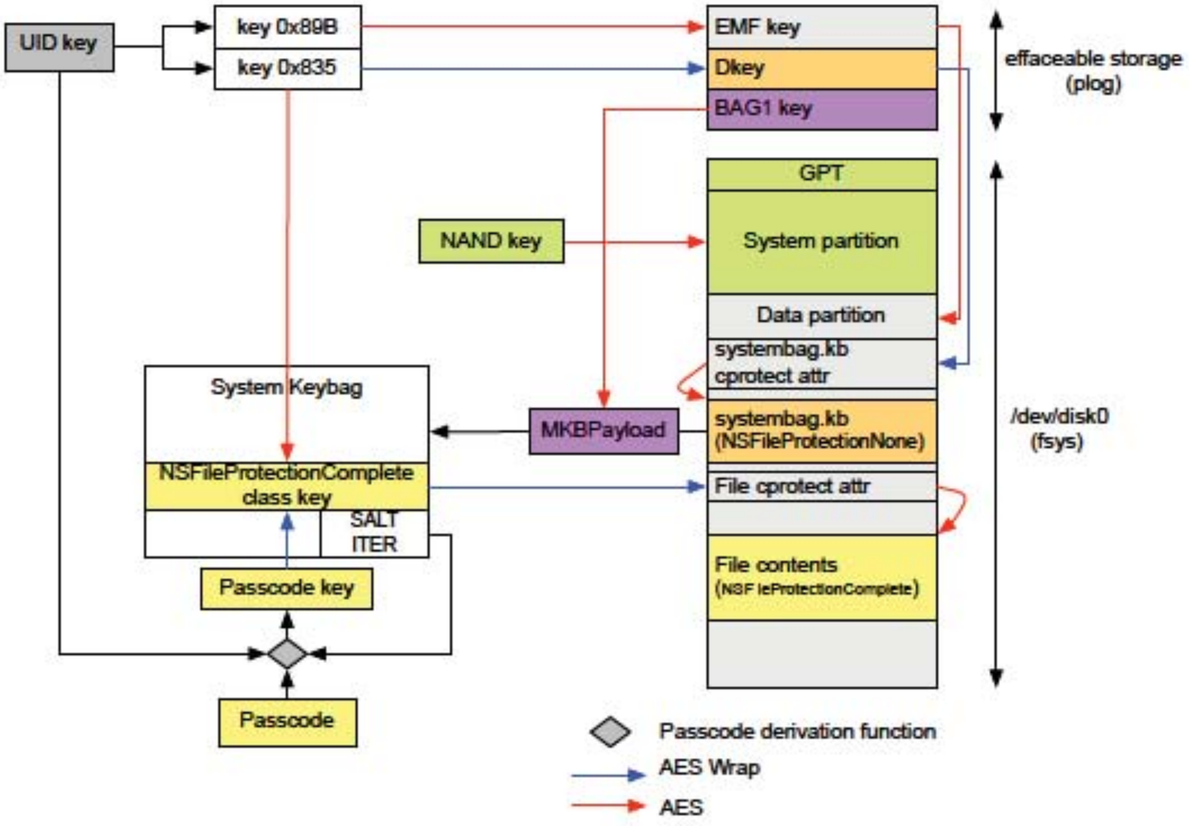
- boot : Low Level Bootloader (LLB) image
- plog : Effaceable area
- nvrm : nvram, contains environments variables
- firm : iBoot, device tree, boot logos (IMG3 images)
- fsys : Filesystem partition, mapped as /dev/disk0

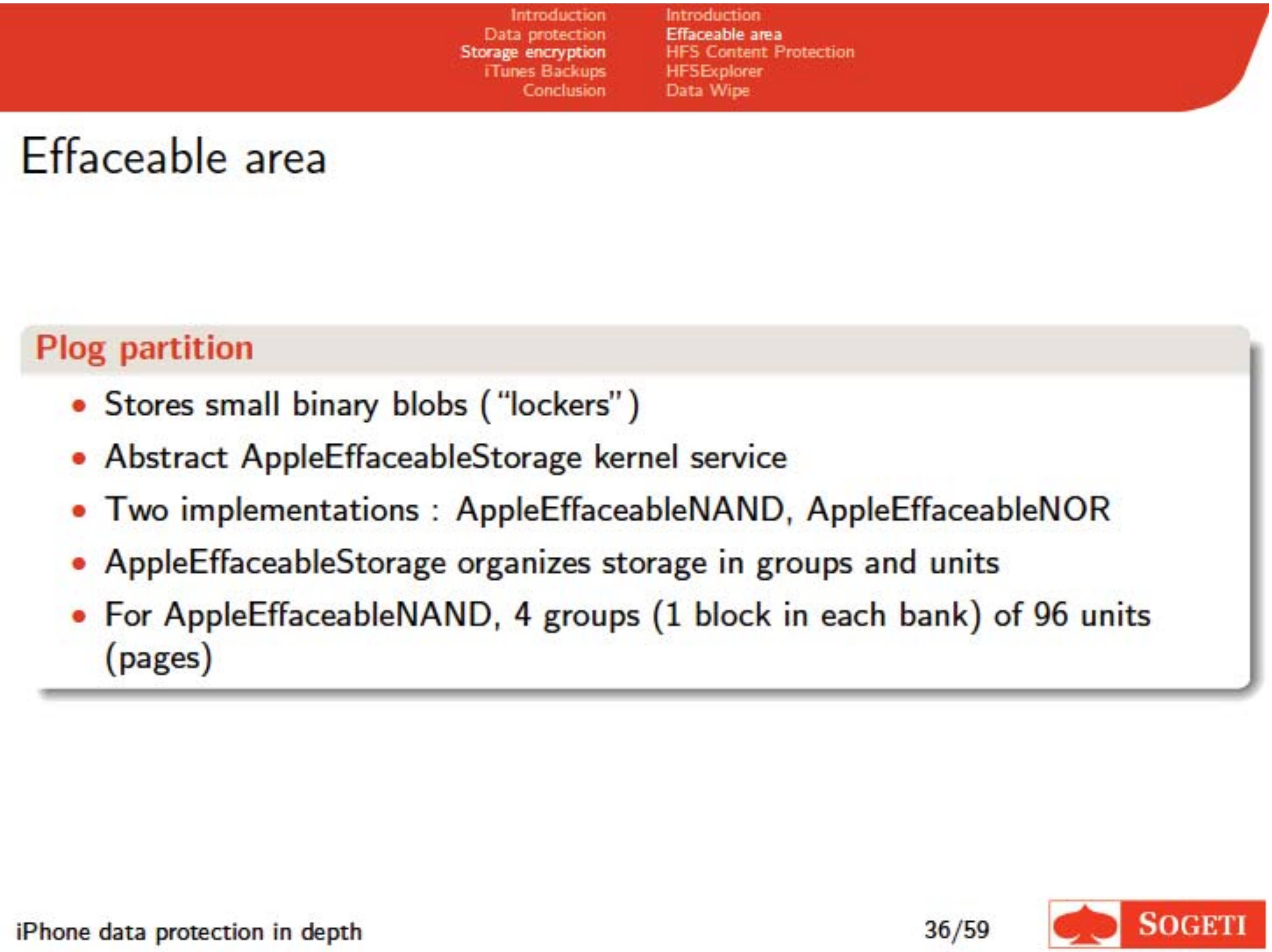
16 Gb iPhone 4 NAND layout

boot	plog	nvrm	firm	fsys	reserved
block 0	block 1	blocks 2 - 7	blocks 8 - 15	blocks 16 - 4084	blocks 4085 - 4100

- 4 banks of 4100 blocks of 128 pages of 8192 bytes data, 448 bytes spare

iOS 4 Storage encryption overview

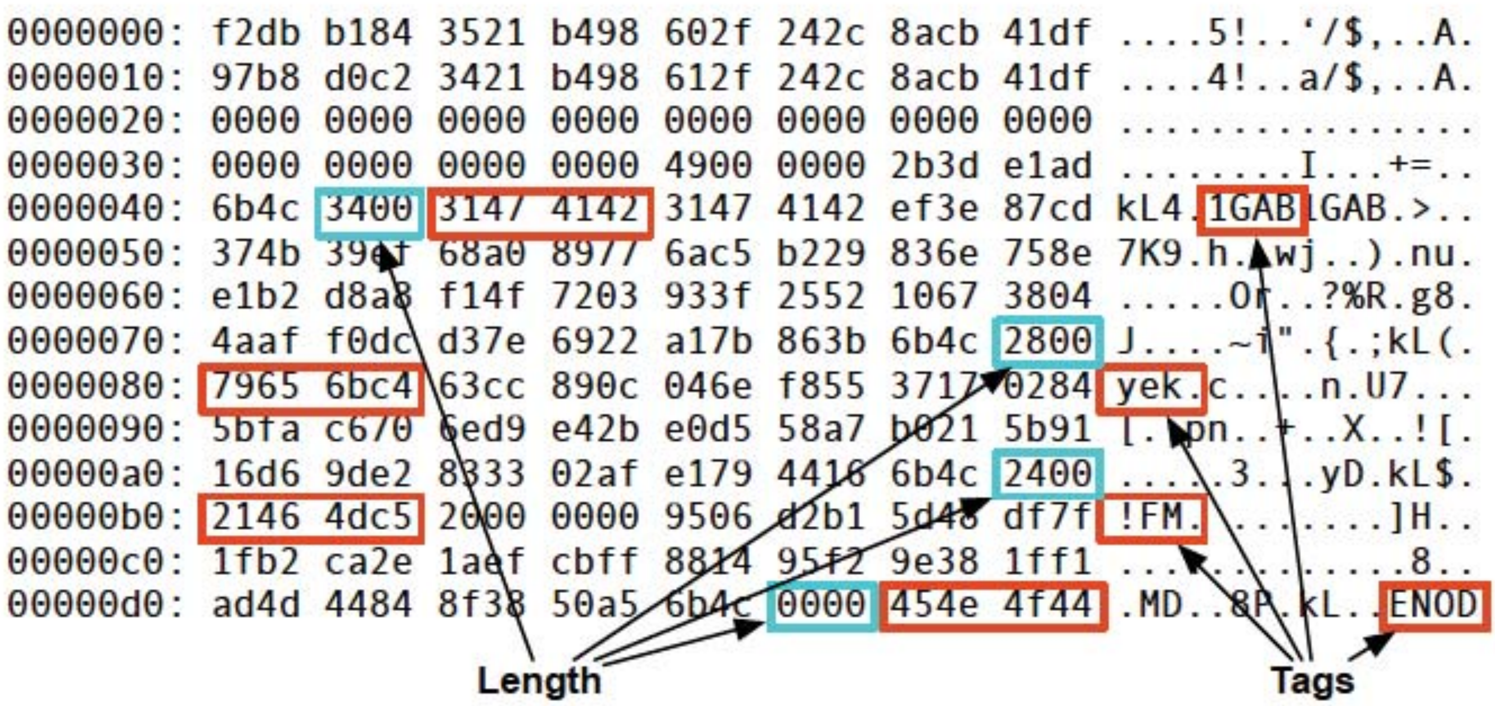




Effaceable area

Plog partition

- Stores small binary blobs ("lockers")
- Abstract AppleEffaceableStorage kernel service
- Two implementations : AppleEffaceableNAND, AppleEffaceableNOR
- AppleEffaceableStorage organizes storage in groups and units
- For AppleEffaceableNAND, 4 groups (1 block in each bank) of 96 units (pages)



```
0000000: f2db b184 3521 b498 602f 242c 8acb 41df ....5!..'/$,..A.
0000010: 97b8 d0c2 3421 b498 612f 242c 8acb 41df ....4!..a/$,..A.
0000020: 0000 0000 0000 0000 0000 0000 0000 0000 ................
0000030: 0000 0000 0000 0000 4900 0000 2b3d e1ad ........I...+=..
0000040: 6b4c 3400 3147 4142 3147 4142 ef3e 87cd kL4.1GAB1GAB.>..
0000050: 374b 39ef 68a0 8977 6ac5 b229 836e 758e 7K9.h..wj..).nu.
0000060: e1b2 d8a8 f14f 7203 933f 2552 1067 3804 .....Or..?%R.g8.
0000070: 4aaf f0dc d37e 6922 a17b 863b 6b4c 2800 J....~i".{.;kL(.
0000080: 7965 6bc4 63cc 890c 046e f855 3717 0284 yek.c....n.U7...
0000090: 5bfa c670 6ed9 e42b e0d5 58a7 b021 5b91 [..pn..+..X..![.
00000a0: 16d6 9de2 8333 02af e179 4416 6b4c 2400 .....3...yD.kL$.
00000b0: 2146 4dc5 2000 0000 9506 d2b1 5d48 df7f !FM.........]H..
00000c0: 1fb2 ca2e 1aef cbff 8814 95f2 9e38 1ff1 ..............8..
00000d0: ad4d 4484 8f38 50a5 6b4c 0000 454e 4f44 .MD..8P.kL..ENOD
```

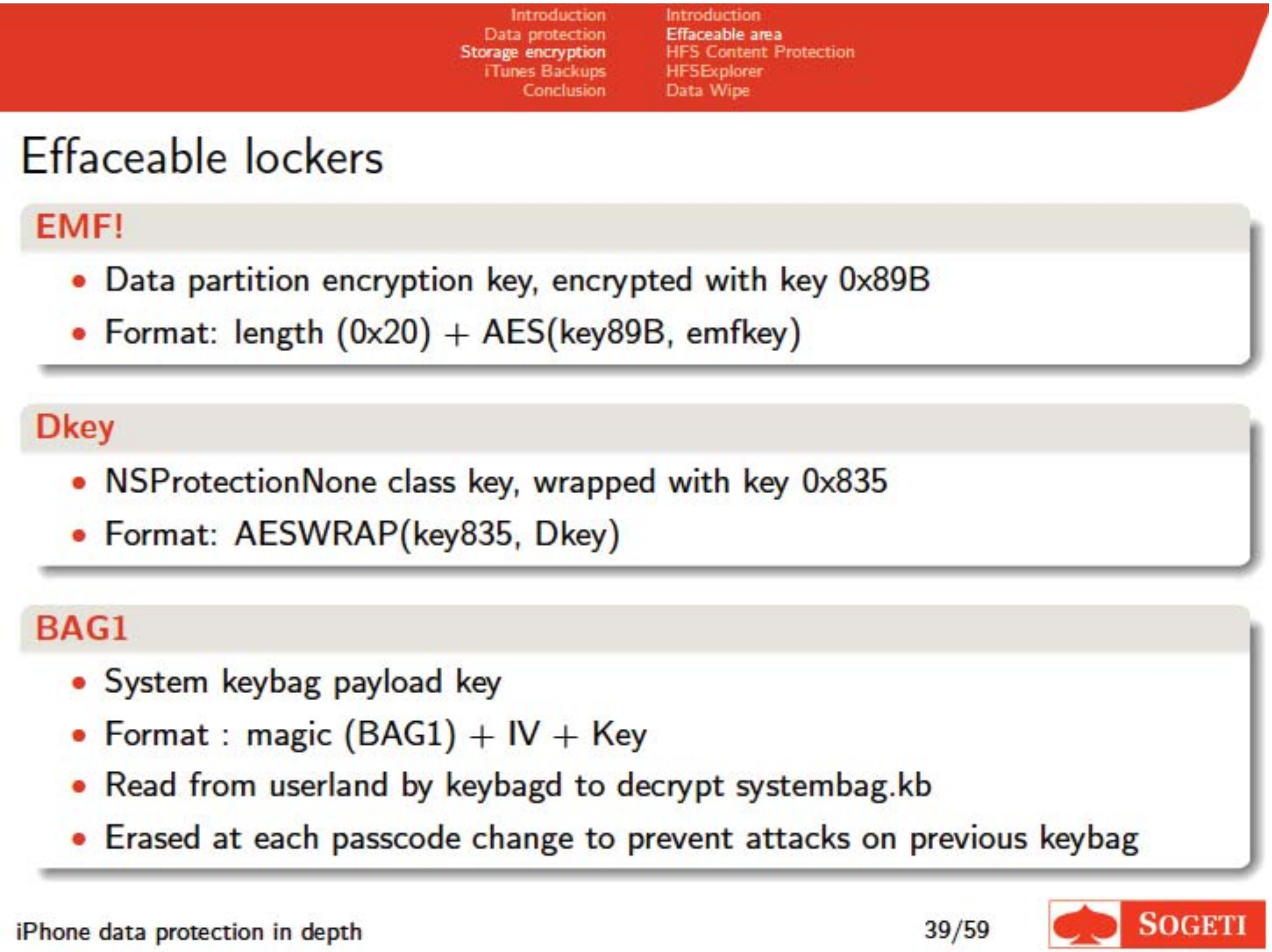
Plog structures

Plog Unit Header

- header[0:16] XOR header[16:31] = 'ecaF' + 0x1 + 0x1 + 0x0
- generation : incremented at each write
- crc32 (headers + data)

Plog lockers format

kL	length	locker tag	locker data



Effaceable lockers

EMF!

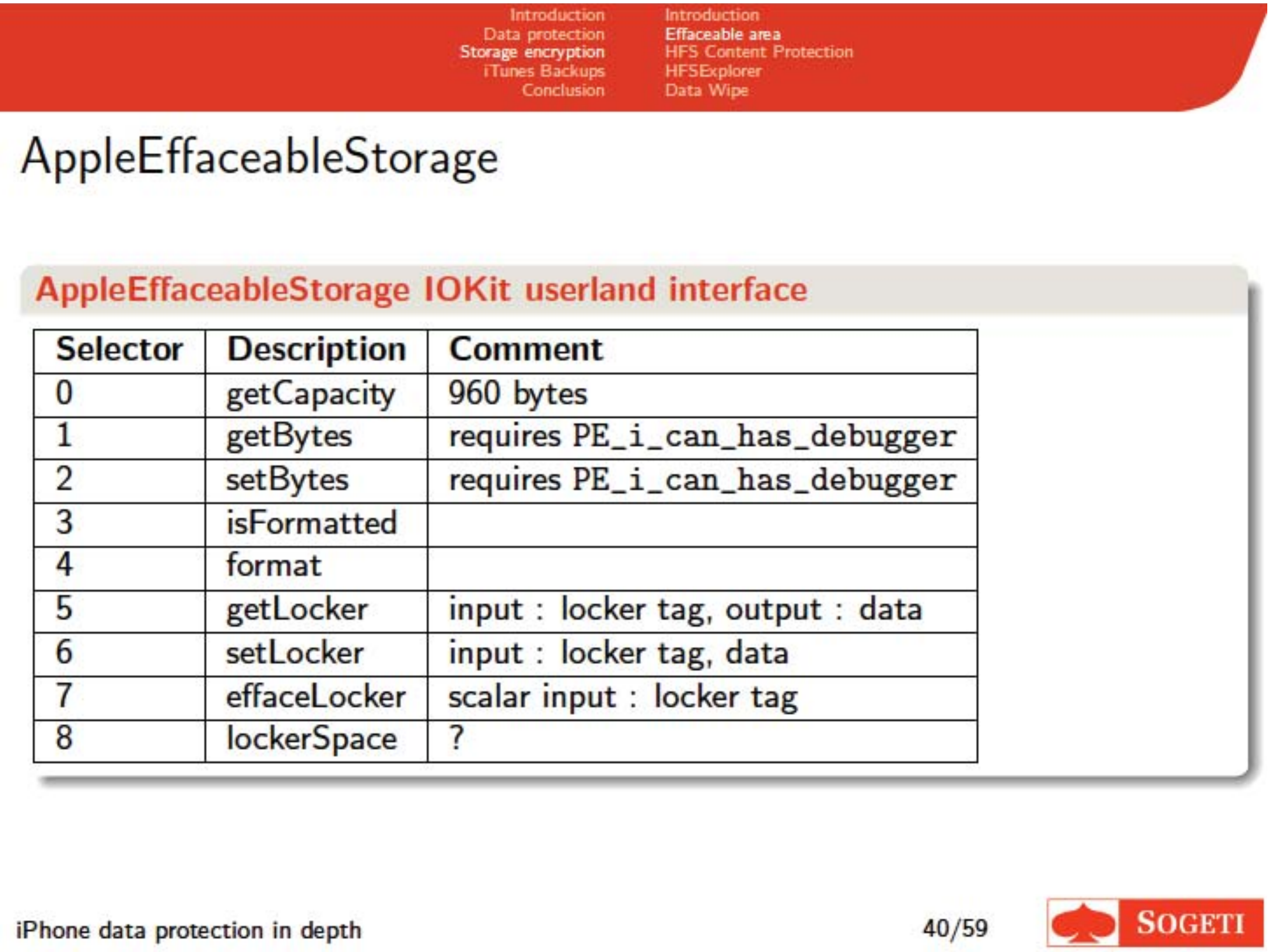
- Data partition encryption key, encrypted with key 0x89B
- Format: length (0x20) + AES(key89B, emfkey)

Dkey

- NSProtectionNone class key, wrapped with key 0x835
- Format: AESWRAP(key835, Dkey)

BAG1

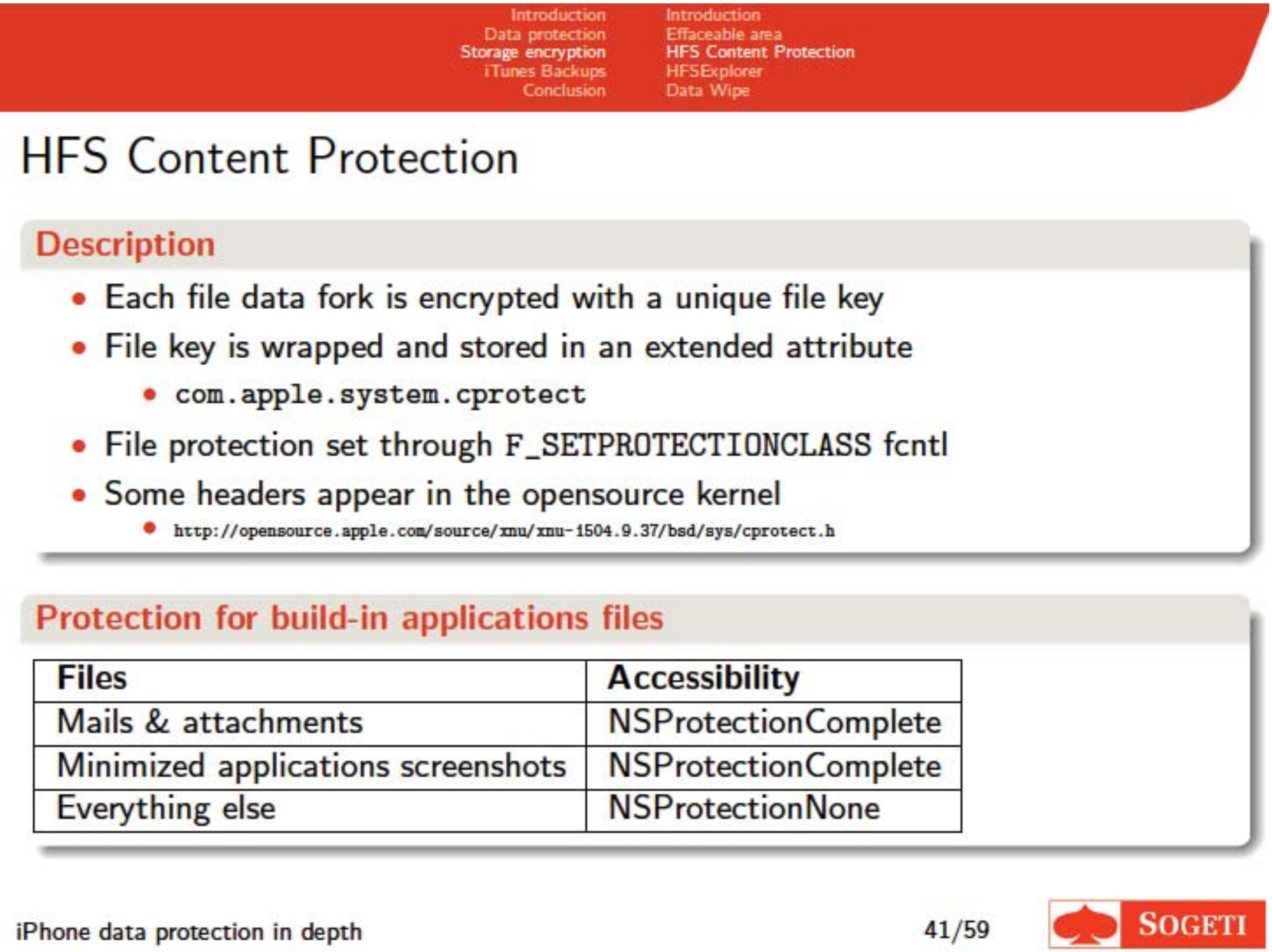
- System keybag payload key
- Format : magic (BAG1) + IV + Key
- Read from userland by keybagd to decrypt systembag.kb
- Erased at each passcode change to prevent attacks on previous keybag



AppleEffaceableStorage

AppleEffaceableStorage IOKit userland interface

Selector	Description	Comment
0	getCapacity	960 bytes
1	getBytes	requires PE_i_can_has_debugger
2	setBytes	requires PE_i_can_has_debugger
3	isFormatted	
4	format	
5	getLocker	input : locker tag, output : data
6	setLocker	input : locker tag, data
7	effaceLocker	scalar input : locker tag
8	lockerSpace	?



HFS Content Protection

Description

- Each file data fork is encrypted with a unique file key
- File key is wrapped and stored in an extended attribute
  - `com.apple.system.cprotect`
- File protection set through `F_SETPROTECTIONCLASS` fcntl
- Some headers appear in the opensource kernel
  - `http://opensource.apple.com/source/xnu/xnu-1504.9.37/bsd/sys/cprotect.h`

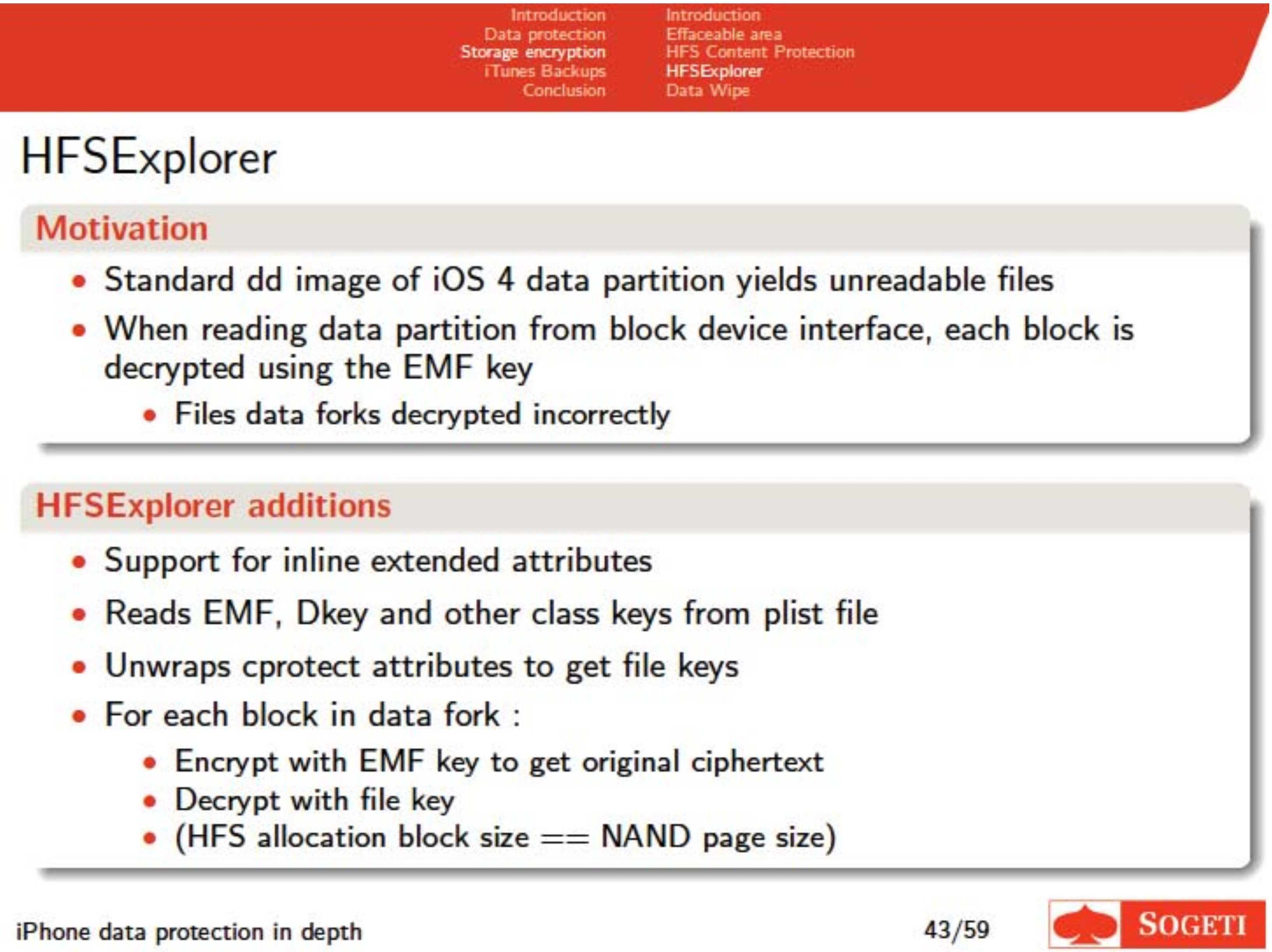
Protection for build-in applications files

Files	Accessibility
Mails & attachments	NSProtectionComplete
Minimized applications screenshots	NSProtectionComplete
Everything else	NSProtectionNone

HFS Content Protection

cprotect extended attribute format

```
struct cprotect_xattr
{
    uint16_t xattr_version; // =2 (version?)
    uint16_t zero; // =0
    uint32_t unknown; // leaks stack dword in one code path :)
    uint32_t protection_class_id;
    uint32_t wrapped_length; // 40 bytes (32 + 8 bytes from
                             // aes wrap integrity)
    uint8_t wrapped_key[1]; // wrapped_length
};
```



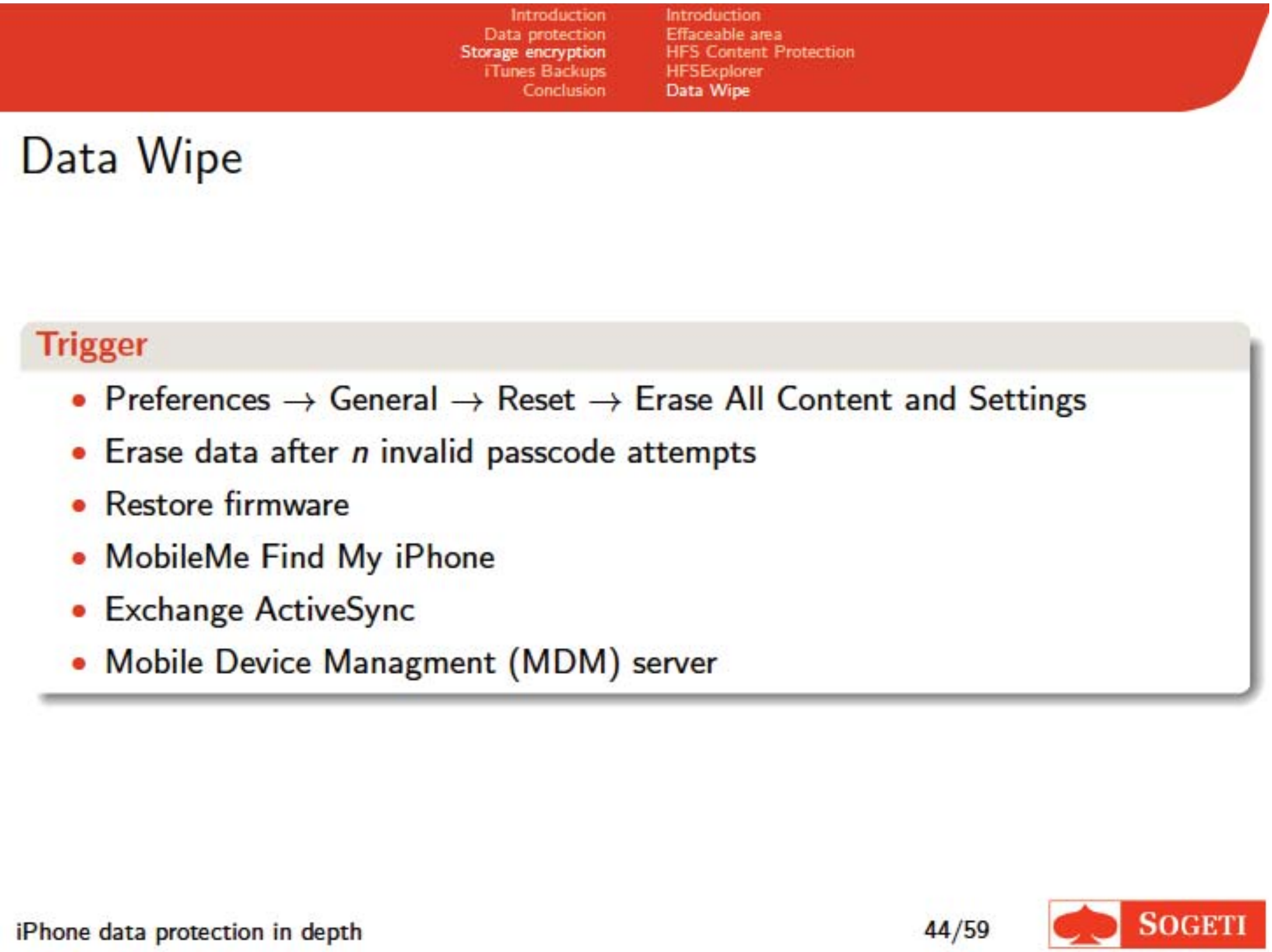
HFSExplorer

Motivation

- Standard dd image of iOS 4 data partition yields unreadable files
- When reading data partition from block device interface, each block is decrypted using the EMF key
  - Files data forks decrypted incorrectly

HFSExplorer additions

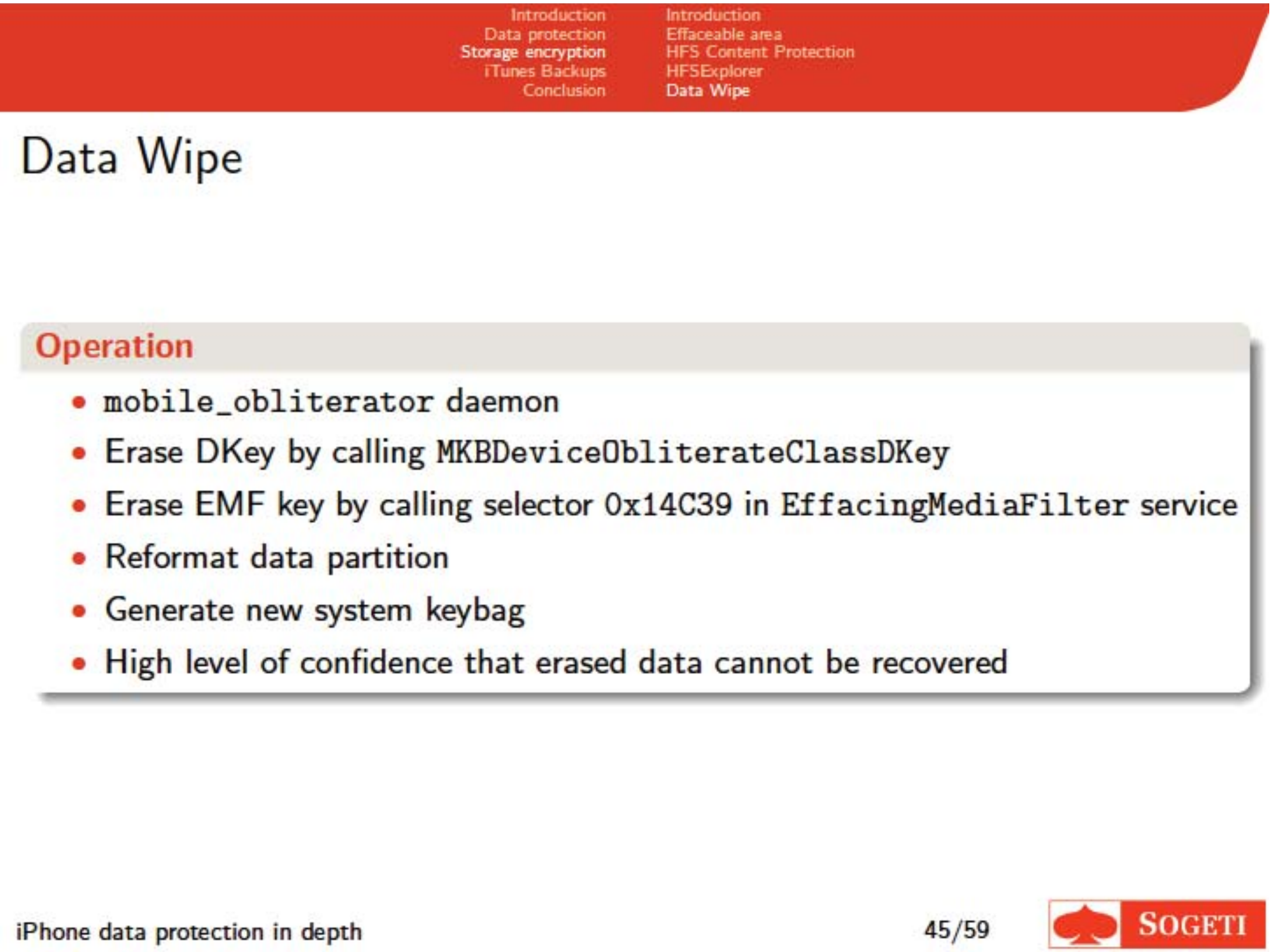
- Support for inline extended attributes
- Reads EMF, Dkey and other class keys from plist file
- Unwraps cprotect attributes to get file keys
- For each block in data fork :
  - Encrypt with EMF key to get original ciphertext
  - Decrypt with file key
  - (HFS allocation block size == NAND page size)



Data Wipe

Trigger

- Preferences → General → Reset → Erase All Content and Settings
- Erase data after *n* invalid passcode attempts
- Restore firmware
- MobileMe Find My iPhone
- Exchange ActiveSync
- Mobile Device Managment (MDM) server

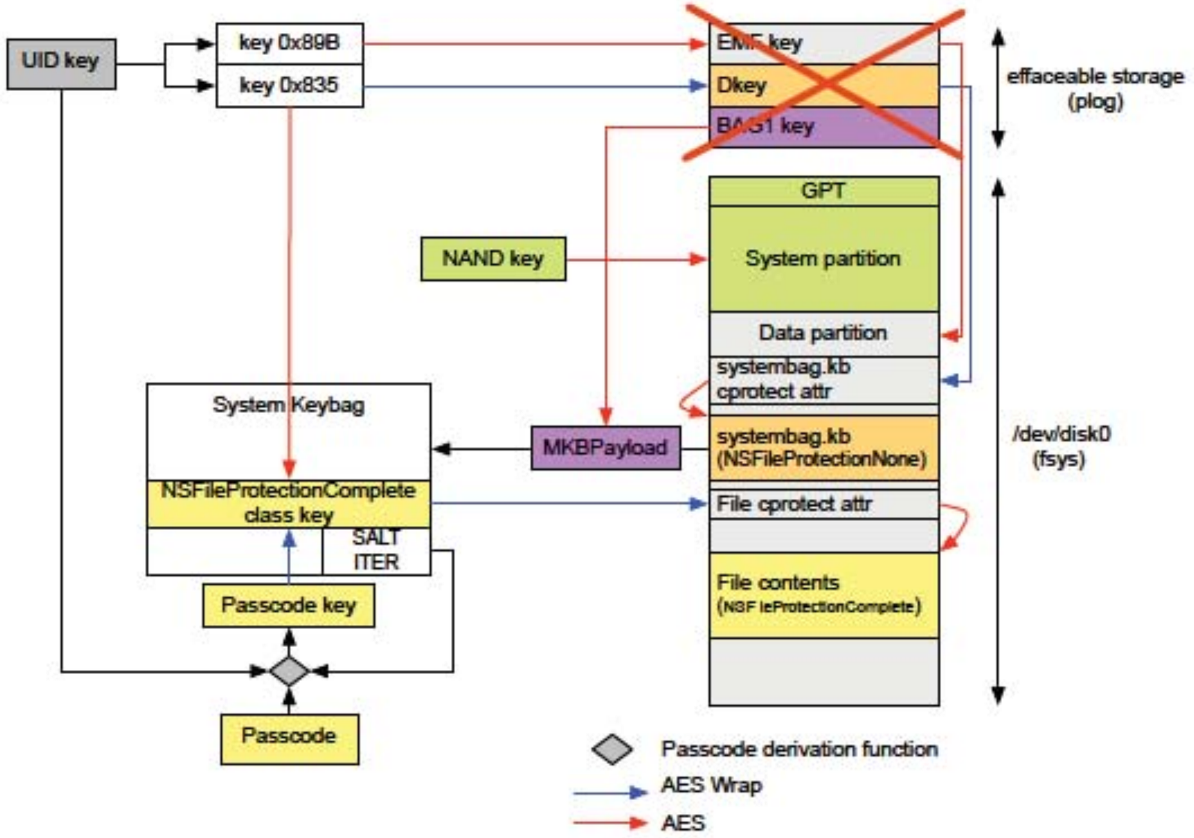


Data Wipe

Operation

- `mobile_obliterator` daemon
- Erase DKey by calling `MKBDeviceObliterateClassDKey`
- Erase EMF key by calling selector `0x14C39` in `EffacingMediaFilter` service
- Reformat data partition
- Generate new system keybag
- High level of confidence that erased data cannot be recovered

iOS 4 Data wipe



Plan

1 Introduction

2 Data protection

3 Storage encryption

4 iTunes Backups
- Files format
- Keybag format
- Keychain format
- iTunes backup decrypter

5 Conclusion

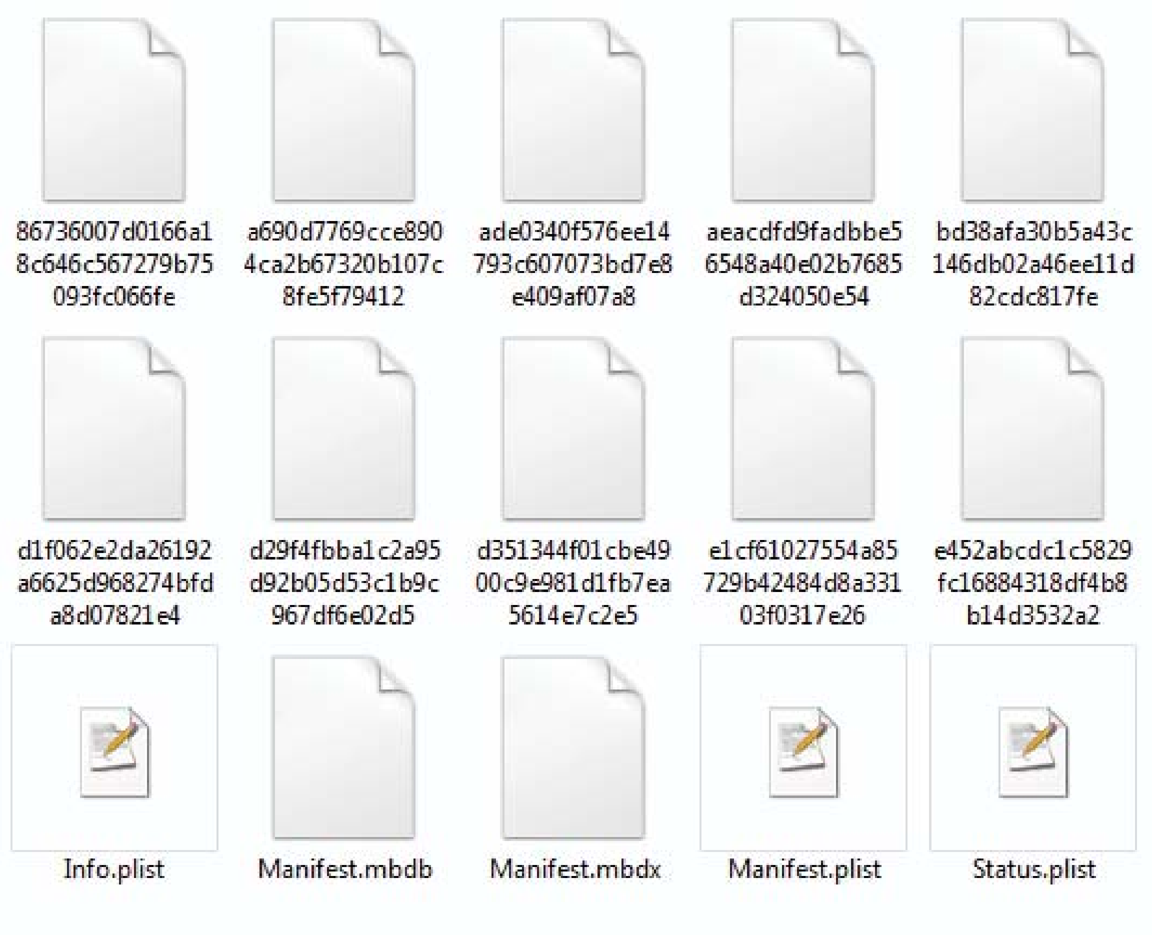
Backed up files

Backup storage

- One directory per backup
- `%APPDATA%/Apple Computer/MobileSync/Backup/<udid>`
- **Can be password protected**
- Each file stored in a separate file
  - Encrypted (AES-256 CBC)
  - Filenames : SHA1 hashes

Database: MBDB

- Custom format
- Two files: `Manifest.mbdb`, `Manifest.mbdx`
- Contains information to restore files correctly
  - Filenames, size, permissions, extended attributes, etc.



86736007d0166a18c646c567279b75093fc066fe

a690d7769cce8904ca2b67320b107c8fe5f79412

ade0340f576ee14793c607073bd7e8e409af07a8

aeacdfd9fadbbe56548a40e02b7685d324050e54

bd38afa30b5a43c146db02a46ee11d82cdc817fe

d1f062e2da26192a6625d968274bfda8d07821e4

d29f4fbba1c2a95d92b05d53c1b9c967df6e02d5

d351344f01cbe4900c9e981d1fb7ea5614e7c2e5

e1cf61027554a85729b42484d8a33103f0317e26

e452abcdc1c5829fc16884318df4b8b14d3532a2

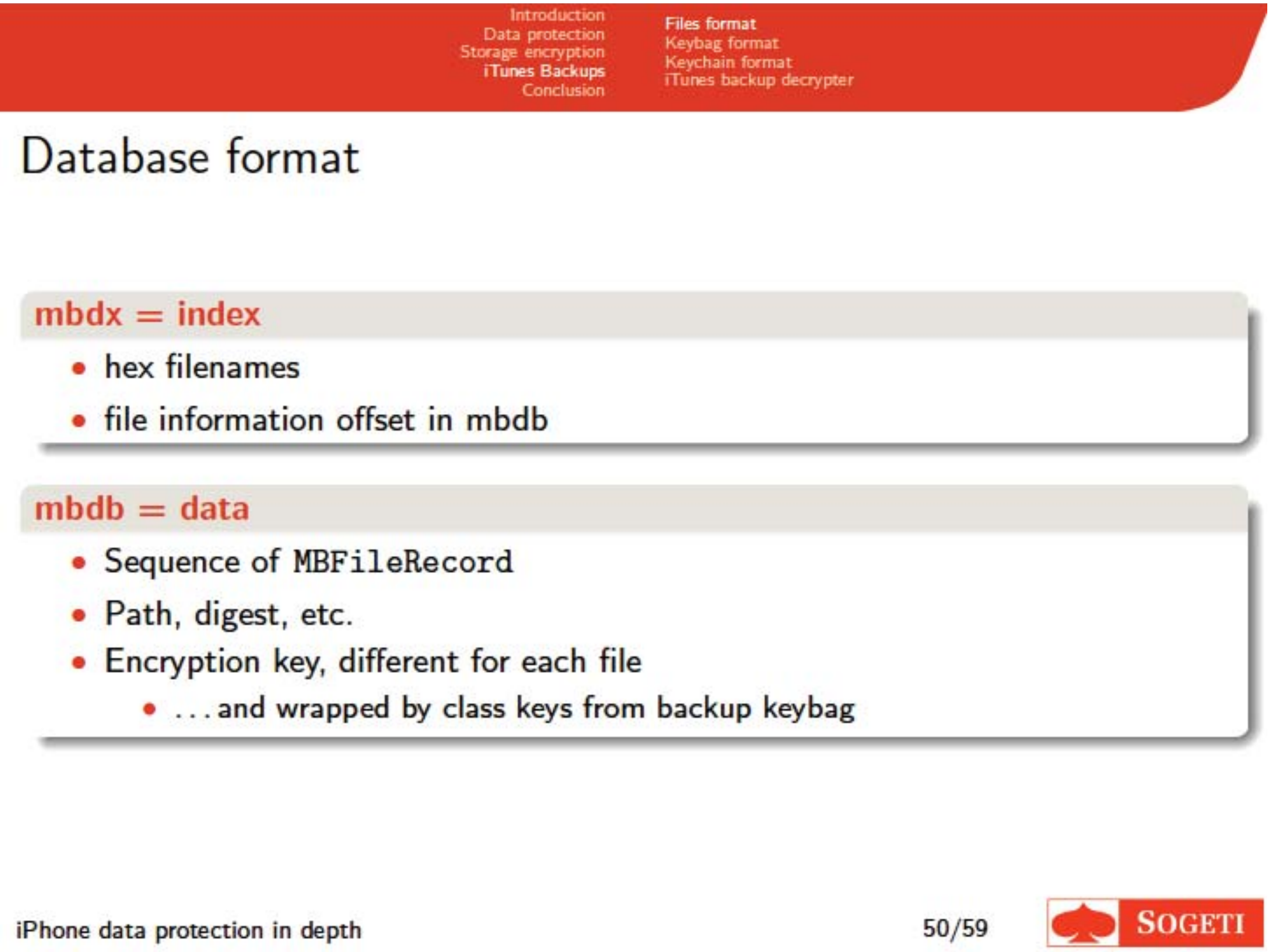
Info.plist

Manifest.mbdb

Manifest.mbdx

Manifest.plist

Status.plist



Database format

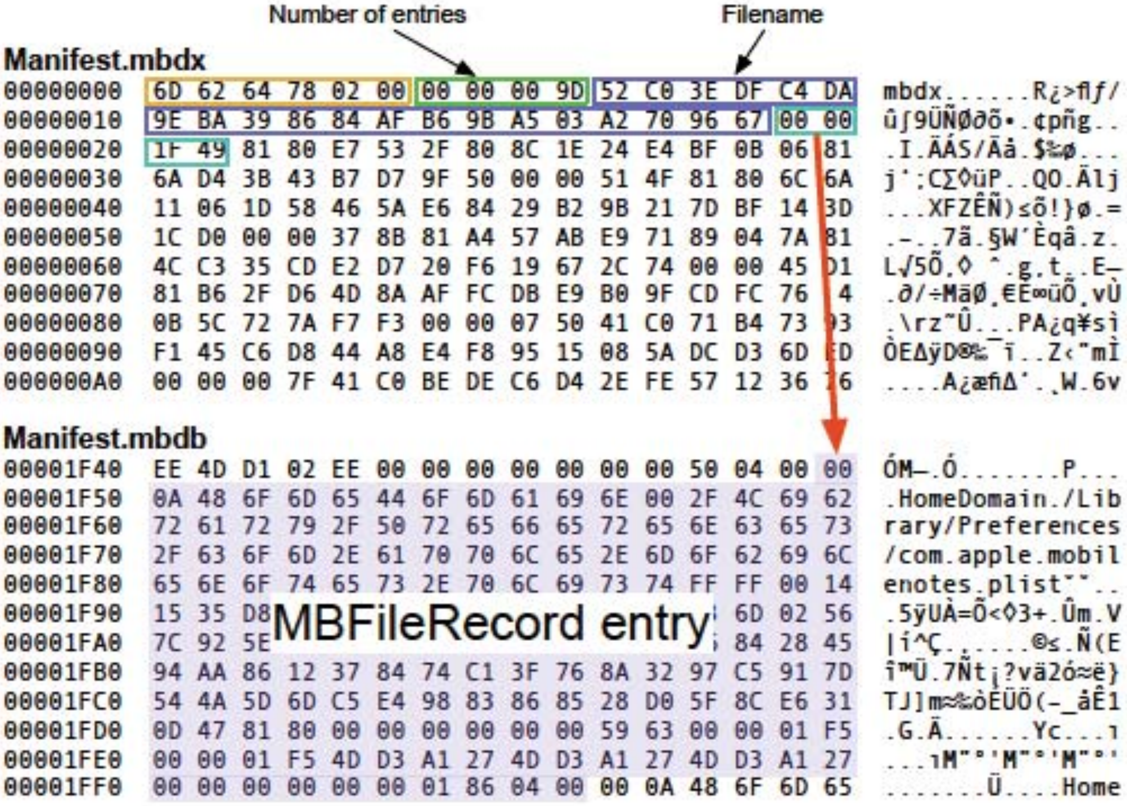
mbdx = index

- hex filenames
- file information offset in mbdb

mbdb = data

- Sequence of `MBFileRecord`
- Path, digest, etc.
- Encryption key, different for each file
  - . . . and wrapped by class keys from backup keybag

Database format



Manifest.mbdx

```
00000000  6D 62 64 78 02 00 00 00 00 9D 52 C0 3E DF C4 DA  mbdx......R¿>ﬂƒ/
00000010  9E BA 39 86 84 AF B6 9B A5 03 A2 70 96 67 00 00  û∫9ÜÑØ∂õ•.¢pñg..
00000020  1F 49 81 80 E7 53 2F 80 8C 1E 24 E4 BF 0B 06 81  .I.ÄÁS/Äå.$‰ø...
00000030  6A D4 3B 43 B7 D7 9F 50 00 00 51 4F 81 80 6C 6A  j';C∑◊üP..QO.Älj
00000040  11 06 1D 58 46 5A E6 84 29 B2 9B 21 7D BF 14 3D  ...XFZÊÑ)≤õ!}ø.=
00000050  1C D0 00 00 37 8B 81 A4 57 AB E9 71 89 04 7A 81  .–..7ã.§W´Èqâ.z.
00000060  4C C3 35 CD E2 D7 20 F6 19 67 2C 74 00 00 45 D1  L√5Õ‚◊ ˆ.g,t..E—
00000070  81 B6 2F D6 4D 8A AF FC DB E9 B0 9F CD FC 76  4  .∂/÷MäØ˛€È∞üÕ˛vÙ
00000080  0B 5C 72 7A F7 F3 00 00 07 50 41 C0 71 B4 73 93  .\rz˜Û...PA¿q¥sì
00000090  F1 45 C6 D8 44 A8 E4 F8 95 15 08 5A DC D3 6D  D  ÒEΔÿD®‰¯ï..Z‹"mÌ
000000A0  00 00 00 7F 41 C0 BE DE C6 D4 2E FE 57 12 36  6  ....A¿æﬁΔ'.˛W.6v
```

Manifest.mbdb

```
00001F40  EE 4D D1 02 EE 00 00 00 00 00 00 00 50 04 00 00  ÓM—.Ó.......P...
00001F50  0A 48 6F 6D 65 44 6F 6D 61 69 6E 00 2F 4C 69 62  .HomeDomain./Lib
00001F60  72 61 72 79 2F 50 72 65 66 65 72 65 6E 63 65 73  rary/Preferences
00001F70  2F 63 6F 6D 2E 61 70 70 6C 65 2E 6D 6F 62 69 6C  /com.apple.mobil
00001F80  65 6E 6F 74 65 73 2E 70 6C 69 73 74 FF FF 00 14  enotes.plist˘˘..
00001F90  15 35 D8                            6D 02 56  .5ÿUÀ=Õ<◊3+.Ûm.V
00001FA0  7C 92 5E                            84 28 45  |í^Ç.......©≤.Ñ(E
00001FB0  94 AA 86 12 37 84 74 C1 3F 76 8A 32 97 C5 91 7D  î™Ü.7Ñt¡?vä2ó≈ë}
00001FC0  54 4A 5D 6D C5 E4 98 83 86 85 28 D0 5F 8C E6 31  TJ]m≈‰òÉÜÖ(–_åÊ1
00001FD0  0D 47 81 80 00 00 00 00 00 00 59 63 00 00 01 F5  .G.Ä......Yc...ı
00001FE0  00 00 01 F5 4D D3 A1 27 4D D3 A1 27 4D D3 A1 27  ...ıM"°'M"°'M"°'
00001FF0  00 00 00 00 00 00 01 86 04 00 00 0A 48 6F 6D 65  .......Ü....Home
```

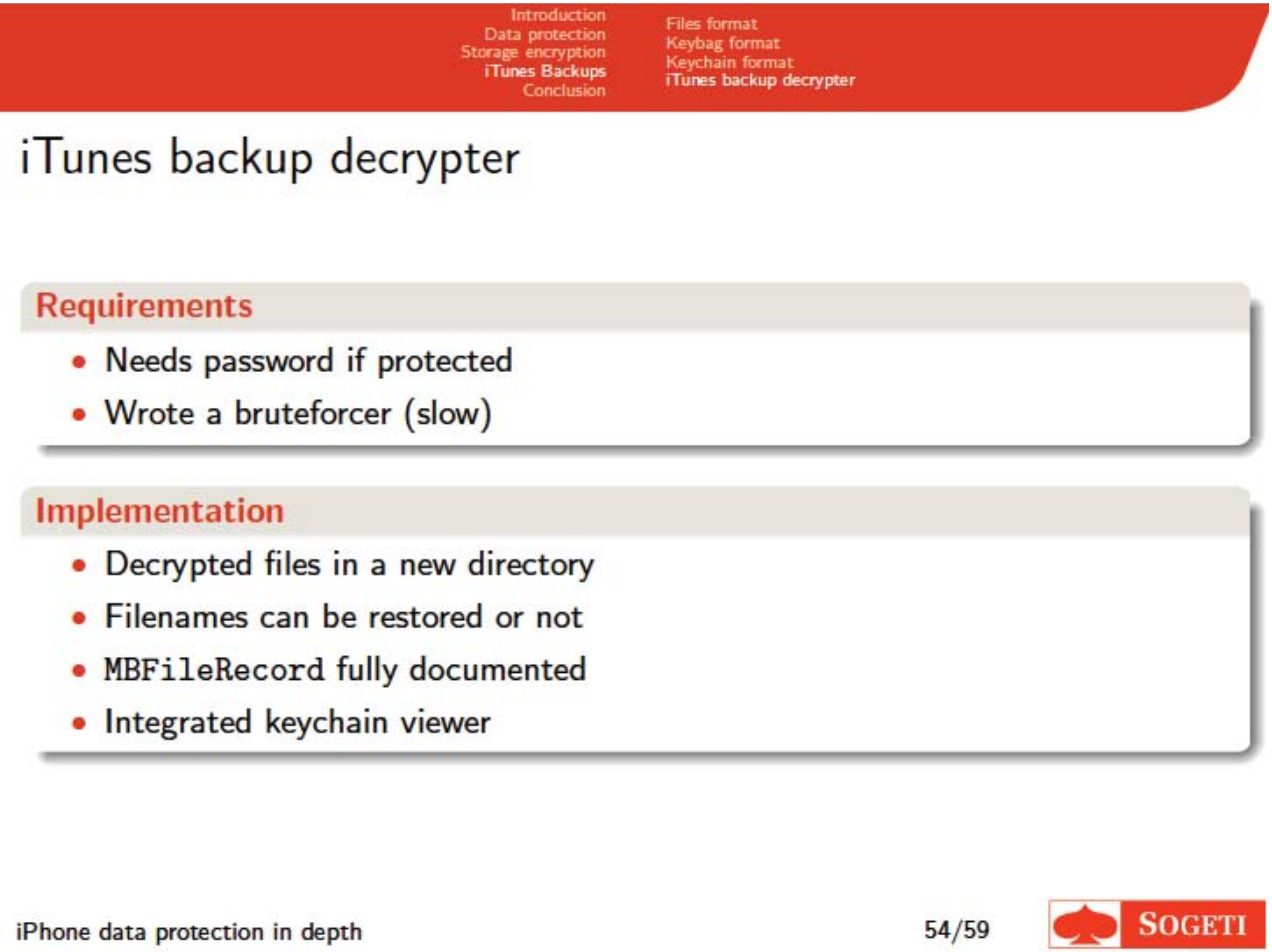
Backup keybag

- Same format as before
- Stored in `Manifest.plist`
  - `BackupKeyBag` section
- Random class keys for each backup
  - Different from system keybag keys

Not all the keys can be retrieved

Backup keychain

- Stored in `keychain-backup.plist`
- Same structure as `keychain-2.db`, but in a plist
- Before accessing it:
  - Backup needs to be decrypted
  - Filenames need to be recovered
- Decrypt items using keychain class keys from backup keybag



iTunes backup decrypter

Requirements

- Needs password if protected
- Wrote a bruteforcer (slow)

Implementation

- Decrypted files in a new directory
- Filenames can be restored or not
- `MBFileRecord` fully documented
- Integrated keychain viewer

Plan

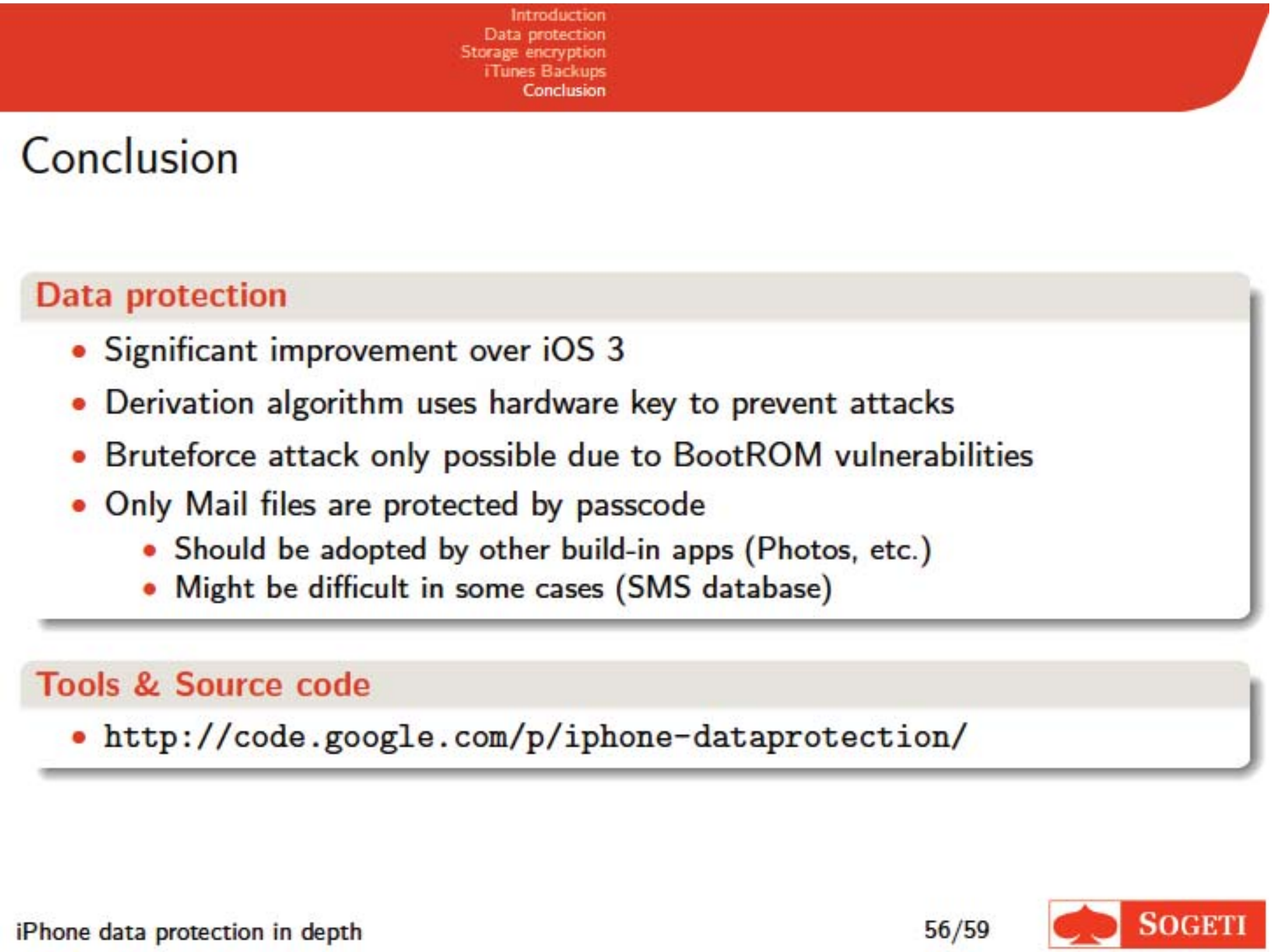
1 Introduction

2 Data protection

3 Storage encryption

4 iTunes Backups

5 Conclusion



Conclusion

Data protection

- Significant improvement over iOS 3
- Derivation algorithm uses hardware key to prevent attacks
- Bruteforce attack only possible due to BootROM vulnerabilities
- Only Mail files are protected by passcode
    - Should be adopted by other build-in apps (Photos, etc.)
    - Might be difficult in some cases (SMS database)

Tools & Source code

- `http://code.google.com/p/iphone-dataprotection/`

Thank you for your attention
Questions ?

References

- Apple WWDC 2010, Session 209 - Securing Application Data
- The iPhone wiki, `http://www.theiphonewiki.com`
- msftguy ssh ramdisk `http://msftguy.blogspot.com/`
- AES wrap, RFC 3394 `http://www.ietf.org/rfc/rfc3394.txt`
- NAND layout, CPICH `http://theiphonewiki.com/wiki/index.php?title=NAND`
- HFSExplorer, Erik Larsson `http://www.catacombae.org/hfsx.html`
- syringe, Chronic dev team `https://github.com/Chronic-Dev/syringe`
- cyanide, Chronic dev team `https://github.com/Chronic-Dev/cyanide`
- usbmux enable code, comex `https://github.com/comex/bloggy/wiki/Redsn0w%2Busbmux`
- restored_pwn, Gojohnnyboi `https://github.com/Gojohnnyboi/restored_pwn`

References

- xpwn crypto tool, planetbeing `https://github.com/planetbeing/xpwn`
- iPhone backup browser
  `http://code.google.com/p/iphonebackupbrowser/`

Exhibit 18

Cellebrite Physical Extraction Manual for iPhone & iPad

July 3rd, 2011

Revision 1.3

cellebrite
mobile data secured

Table of Contents

Introduction

This manual provides an overview of the steps required to extract data from an iPhone or iPad using the UFED Physical Analyzer.

The UFED Physical Analyzer allows you to extract, decode and analyze the following devices running iOS version 3.0 or higher:

- **iPhone (original)**
- **iPhone 3G**
- **iPhone 3GS**
- **iPhone 4 GSM**
- **iPhone 4 CDMA**
- **iPad 1**

Before You Start

You will need:

- A UFED Physical Analyzer installed on a PC with Windows XP/Vista/7 Operating Systems (iPhone/iPad physical extraction is not designed to be used in Virtual Machine environments).
- An iPhone or iPad.
- UFED Cable Number 110.

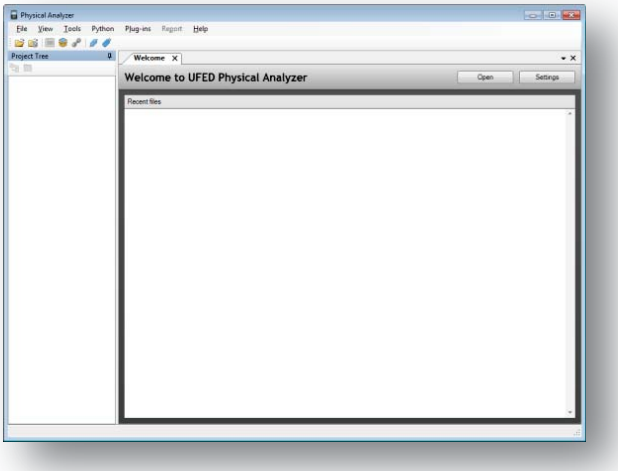
An Internet connection is required before the first use for the installation of updates. Access to the Internet is used to download relevant software and may be carried out through any computer with Internet connection.

Performing an Extraction

The following steps will guide you through the extraction process.

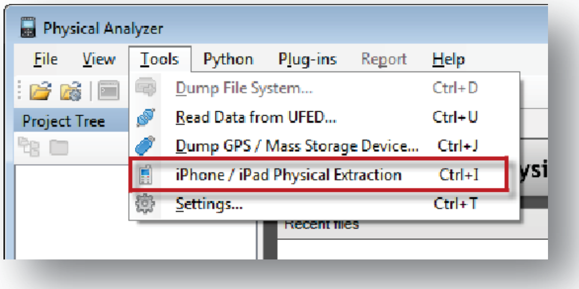
Step 1: Launch the UFED Physical Analyzer

1. Launch UFED Physical Analyzer by clicking the application icon or program shortcut. The default location of UFED Physical Analyzer is: C:\Program Files\Cellebrite Mobile Synchronization\UFED Physical Analyzer.


Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
Welcome
Welcome to UFED Physical Analyzer
Open
Settings
Recent files

Step 2: Open iPhone / iPad Physical Extraction

1. Click the *Tools* menu and click *iPhone/iPad Physical Extraction.* "UFED iPhone Physical" will then launch.


Physical Analyzer
File
View
Tools
Python
Plug-ins
Report
Help
Project Tree
Dump File System... Ctrl+D
Read Data from UFED... Ctrl+U
Dump GPS / Mass Storage Device... Ctrl+J
iPhone / iPad Physical Extraction Ctrl+I
Settings... Ctrl+T
Recent files

On first use

On the first use of UFED iPhone Physical you will be required to download the Apple Device Support Package. The support package contains the newest utilities that enable UFED iPhone Physical to be compatible with a variety of devices. The download may take a while, depending on your Internet connection speed.

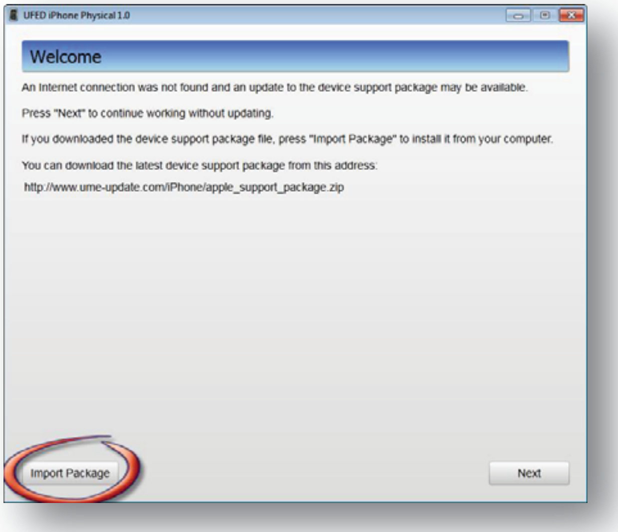
cellebrite
mobile data secured

No Internet connection?

If your computer is not connected to the Internet you can download the support package on a different computer and manually copy it to your computer.

1. Click this link[1] to download the latest Apple Device Support Package:

2. Copy the file to your computer.
3. Click the *Import Package* button and locate the file on your computer.



Welcome

An Internet connection was not found and an update to the device support package may be available.

Press "Next" to continue working without updating.

If you downloaded the device support package file, press "Import Package" to install it from your computer.

You can download the latest device support package from this address:
http://www.ume-update.com/iPhone/apple_support_package.zip

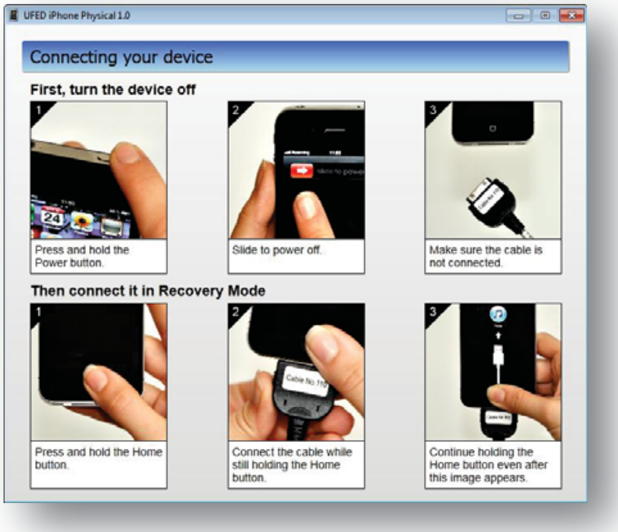
[1] http://www.ume-update.com/iPhone/apple_support_package.zip

cellebrite
mobile data secured

Step 3: Connect the device in Recovery Mode to your PC

1. Follow the steps on the screen to connect the device in Recovery Mode.

   Note: connect your device to the PC using cable # 110 or the iPhone/iPad data cable.



UFED iPhone Physical 1.0

Connecting your device

First, turn the device off

1 Press and hold the Power button.

2 Slide to power off.

3 Make sure the cable is not connected.

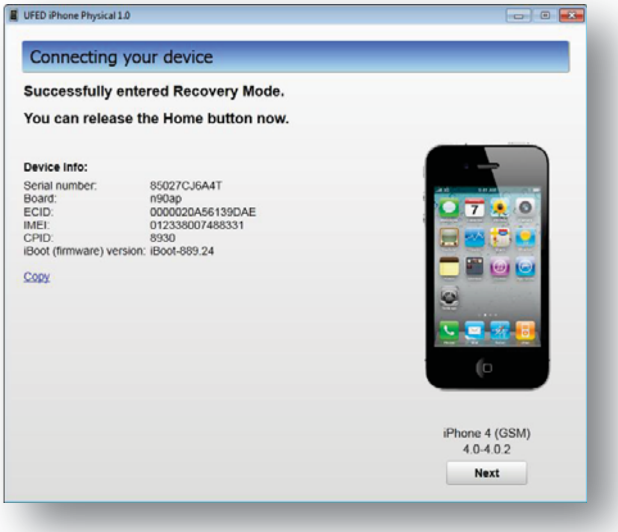
Then connect it in Recovery Mode

1 Press and hold the Home button.

2 Connect the cable while still holding the Home button.

3 Continue holding the Home button even after this image appears.

2. After connecting the device in Recovery Mode, UFED iPhone Physical will display certain device information, such as serial number, IMEI, hardware version, iOS version and more. You can copy that information to the clipboard by clicking the *Copy* link.



Connecting your device

Successfully entered Recovery Mode.

You can release the Home button now.

Device Info:

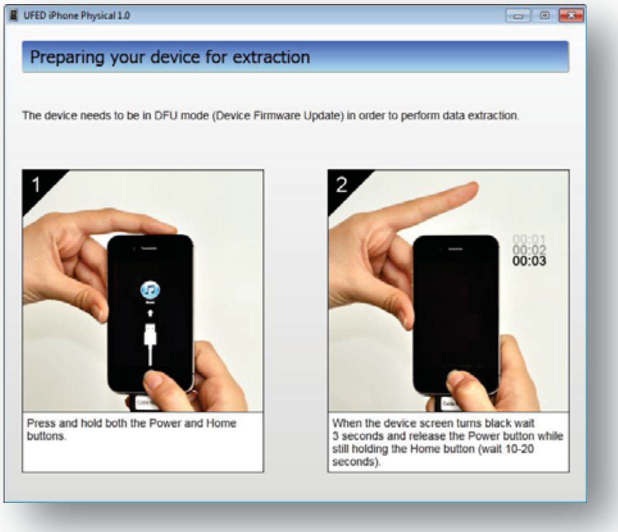
Serial number:	85027CJ6A4T
Board:	n90ap
ECID:	0000020A56139DAE
IMEI:	012338007488331
CPID:	8930
iBoot (firmware) version:	iBoot-889.24

Note: In case a range of versions are displayed, the version of the specific device connected may be any version within the displayed range. In the example above the iOS version may be 4.0, 4.0.1 or 4.0.2.

cellebrite
mobile data secured

Step 4: Setting the Device to DFU Mode

1. Click *Next* on the screen with the device info.
2. Follow the instructions on the screen to set the device to DFU (Device Firmware Upgrade) mode. Be assured that UFED iPhone Physical will not affect the device firmware or user data.



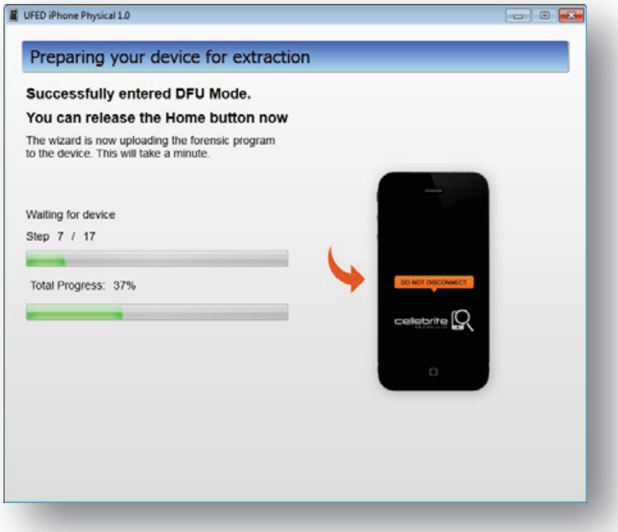
Preparing your device for extraction

The device needs to be in DFU mode (Device Firmware Update) in order to perform data extraction.

1. Press and hold both the Power and Home buttons.

2. When the device screen turns black wait 3 seconds and release the Power button while still holding the Home button (wait 10-20 seconds).

3. When you have succeeded, the following screen will be displayed.



Preparing your device for extraction

Successfully entered DFU Mode.

You can release the Home button now

The wizard is now uploading the forensic program to the device. This will take a minute.

Waiting for device

Step 7 / 17

Total Progress: 37%

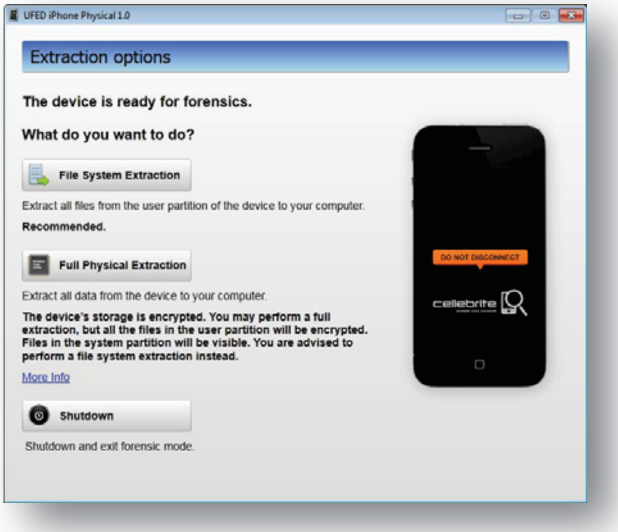
UFED iPhone Physical will upload the forensics program required to extract data from the device. As mentioned above, this will not affect the data, memory or firmware of the device.

cellebrite
mobile data secured

Step 5: Extract Data

Now the device is ready for forensic extraction.

1. Choose the desired extraction method (Full Physical or File System). We recommend reading the Extraction and Encryption FAQ appendix to make the best of your iPhone and iPad extraction.
2. Choose the location you wish to save the extraction to. You can save it on your computer or on a removable storage device.



UFED iPhone Physical 1.0

Extraction options

The device is ready for forensics.

What do you want to do?

File System Extraction

Extract all files from the user partition of the device to your computer.

Recommended.

Full Physical Extraction

Extract all data from the device to your computer.

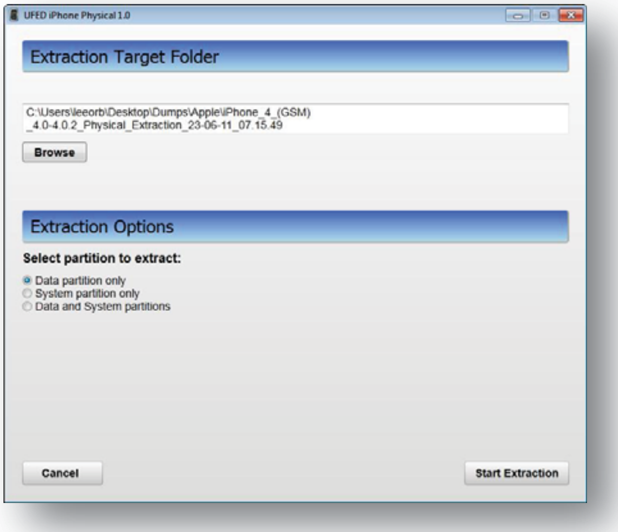
The device's storage is encrypted. You may perform a full extraction, but all the files in the user partition will be encrypted. Files in the system partition will be visible. You are advised to perform a file system extraction instead.

More Info

Shutdown

Shutdown and exit forensic mode.

3. While performing Full Physical Extraction, you will be required to choose the relevant partition for extraction. Select the Data partition, System partition or both partitions.
4. Click Start Extraction.



UFED iPhone Physical 1.0

Extraction Target Folder

C:\Users\leeorb\Desktop\Dumps\Apple\iPhone_4_(GSM)
_4.0-4.0.2_Physical_Extraction_23-06-11_07.15.49

Extraction Options

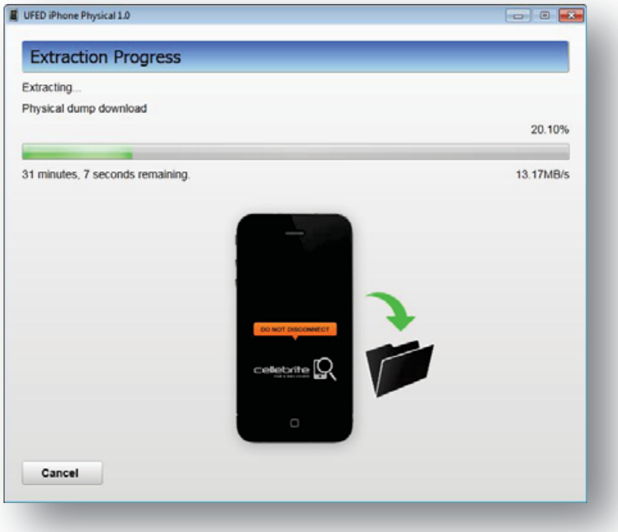
Select partition to extract:

● Data partition only
○ System partition only
○ Data and System partitions

cellebrite
mobile data secured

Step 6: Wait

1. Wait until the extraction is completed. The extraction duration varies depending on the extraction method, the device used, the quantity of data on the device, your computer and other parameters.



Extraction Progress

Extracting...

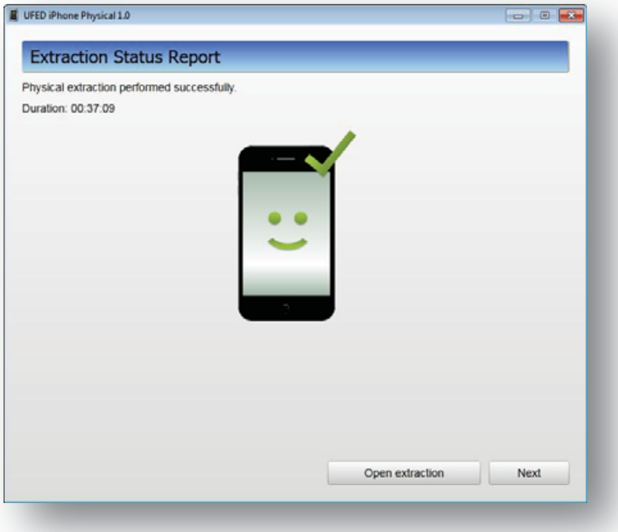
Physical dump download

20.10%

31 minutes, 7 seconds remaining.

13.17MB/s

2. When the extraction is completed you will see this screen.
3. Clicking *Open extraction* will load the extraction file in UFED Physical Analyzer.
4. Clicking *Next* will take you back to the extraction options screen.



UFED iPhone Physical 1.0

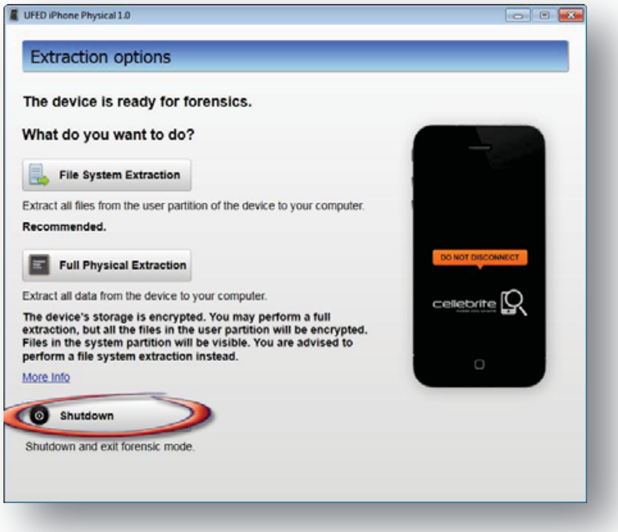
Extraction Status Report

Physical extraction performed successfully.

Duration: 00:37:09

Step 7: Shutdown the Device

1. When extraction is complete, you may click *Shutdown* to safely turn off the device and set it back to normal mode.



The device is ready for forensics.

What do you want to do?

Extract all files from the user partition of the device to your computer.

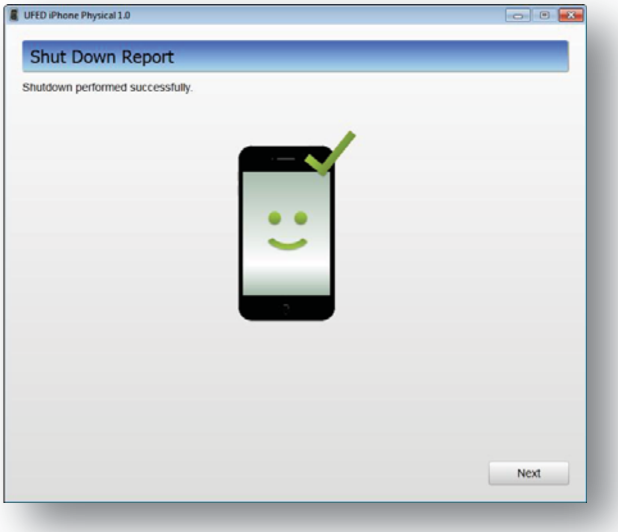
Recommended.

Extract all data from the device to your computer.

The device's storage is encrypted. You may perform a full extraction, but all the files in the user partition will be encrypted. Files in the system partition will be visible. You are advised to perform a file system extraction instead.

Shutdown and exit forensic mode.

2. The *Shut Down Report* screen will indicate your device has successfully been shut down.



Shut Down Report

Shutdown performed successfully.

Appendix - UFED iPhone Physical Extraction and Encryption FAQ

Is it possible to extract data from user locked iPhone devices?

Yes. The UFED iPhone Physical Extraction solution enables extraction of the device image and file system even when user lock is active.

What is "physical extraction"?

Physical extraction is performed by imaging the device’s partitions. This recovers the device's entire file system which can then be decoded by UFED Physical Analyzer. On devices that have data encryption, the contents of the files may be encrypted (explanation below).

What is "low-level file system extraction"?

Apple iOS devices have two partitions: The system partition (normally 1GB) and the user data partition (the rest of the flash memory). The system partition contains the operating system files. The user data partition contains all user-generated content (photos, messages, etc.)

Low-level file system extraction reads the entire directory tree of the user partition and puts it in a simple “tar” file. The user data will not be encrypted in a low-level file system extraction, even if encryption is enabled on the device. However, some "protected" files cannot be fully extracted.

On devices that have data encryption, some files may be protected and inaccessible. Protected files are only readable when the device is turned on regularly and unlocked. Low-level file system extraction cannot extract the contents of those files; only their metadata. Among the protected files are some of the email files.

The system partition is never encrypted, even if encryption is enabled on the device.

What devices have data encryption enabled?

Device	Data Encryption
iPhone (Original), iPhone 3G, iPod Touch 1st and 2nd generation*	Disabled
iPhone 3GS iPod Touch 3rd generation* iPad 1	In some cases. See paragraph below.
iPhone 4 iPod Touch 4th generation* iPad 2*	Enabled

* Extraction from this device is not currently supported.

iPhone 3GS, iPod Touch 3rd Generation and iPad 1 were originally manufactured and shipped with iOS version 3.x. The data encryption feature was added in iOS 4.x.

Simply updating an iOS 3.x device to iOS 4.x (or later) does not enable data encryption. Data encryption will be enabled on these devices only if the user has "restored" the device with iOS 4.x. (or later) "Restore" is a feature in iTunes which reformats the file system (making it encryption-ready) and reinstalls iOS.

If the device had iOS 4.x (or later) preinstalled on it when it was bought, encryption will be enabled.

What type of extracted data will be encrypted?

If data encryption is disabled, all data on the device will be unencrypted and readable. However, if data encryption is enabled, the data that's encrypted varies between the different types of extractions:

Extraction type	If data encryption enabled
Physical extraction - system partition	Will be extracted and not encrypted
Physical extraction - user partition	File contents will be encrypted. Directory tree, file names, modification dates, etc. will not be encrypted
Low-level file system extraction **Non-protected files**	Will be extracted and not encrypted
Low-level file system extraction **Protected files**	File contents will not be extracted. Only 0's will appear. File names, modification dates, etc. will be extracted and not encrypted

What is the best way to extract data from an encrypted device?

The best way to extract data from a device with encryption enabled is to perform a low-level file system extraction. You will be able to retrieve all user content except protected files (among which are some of the email files).

cellebrite
mobile data secured

Can jailbreaking help extract data from an encrypted device?

Unfortunately, jailbreaking does not help circumvent the data encryption. The Cellebrite UFED solution performs extraction without Jailbreaking the device. Both Jailbroken and non-jailbroken devices are supported.

Does data extraction affect the storage or data on the device?

No.

The extraction application does not load iOS, but instead loads a special forensic utility to the device. This utility is loaded to the device's memory (RAM) and runs directly from there. Therefore, it does not modify the device's storage and does not leave any footprints.

Exhibit 19

Cryptographic Services

Cryptographic services form the foundation of securing data in transit (secure communications) and data at rest (secure storage). Using sophisticated mathematics, they allow you to:

- Encrypt and decrypt data so that it cannot be understood by an outside observer
- Verify that data has not been modified since it was originally sent by hashing, signing, and verifying

This chapter describes these cryptographic techniques and briefly summarizes the technologies that OS X and iOS provide to help you use cryptography in your own application.

Encryption and Decryption

Encryption is a means of protecting data from interception by transforming it into a form that is not readable except by someone who knows how to transform it back.

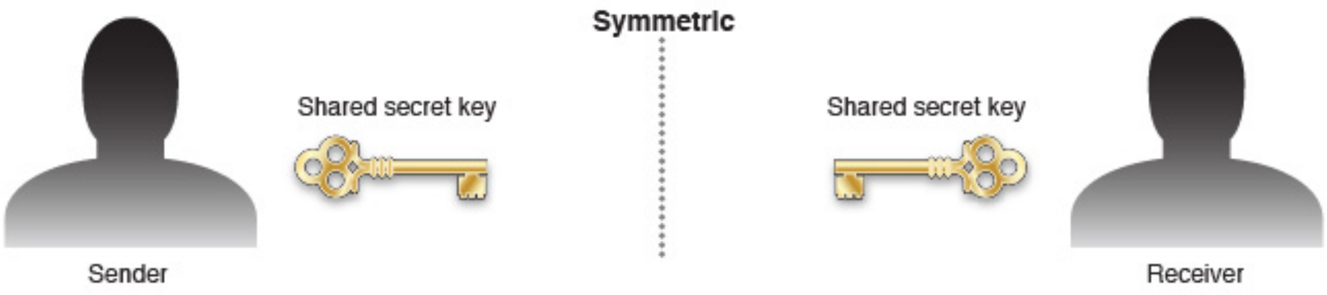
Encryption is commonly used to protect data in transit and data at rest. When information must be sent across an untrusted communication channel, it is the responsibility of the two endpoints to use encryption to secure the communication. Similarly, when storing information on a local disk, an app may use encryption to ensure that the information is not readable by third parties even if the computer is stolen.

There are many different encryption techniques, called *ciphers*, that work in different ways and can serve different purposes. Ciphers generally work by combining the original information (the *cleartext*, or *plaintext*) with a second piece of information (a key) in some fashion to produce an encrypted form, called the *ciphertext*.

Modern encryption techniques can be grouped into three broad categories: symmetric encryption, asymmetric encryption, and steganography.

Symmetric Encryption

In symmetric encryption, a single key (usually a long string of random bytes) is used to mathematically transform a piece of information and is later used in reverse to retrieve the original information.

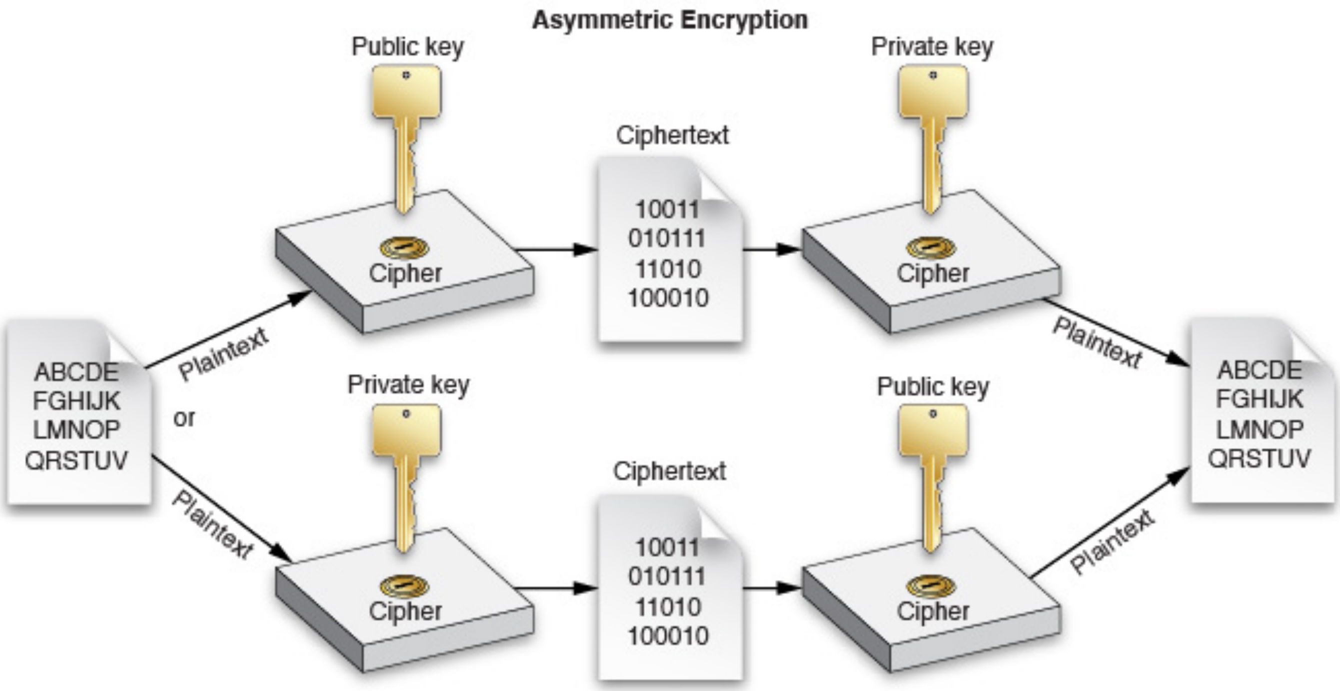


Symmetric encryption is often used for secure communication. However, because both endpoints must know the same secret key, symmetric encryption is not sufficient by itself.

Asymmetric Encryption

In asymmetric encryption, two mathematically related keys are used to transform a piece of information. Information encrypted with one key can be decrypted only with the other key and vice versa. Generally speaking, one of these keys (the private key) is kept secret, and the other key (the public key) is made broadly available. For this reason, asymmetric encryption is also called *public key cryptography*.

> **Note:** Although the two keys are mathematically related, it is considered computationally infeasible to derive one key from the other. The security of public key cryptography depends on this being the case.

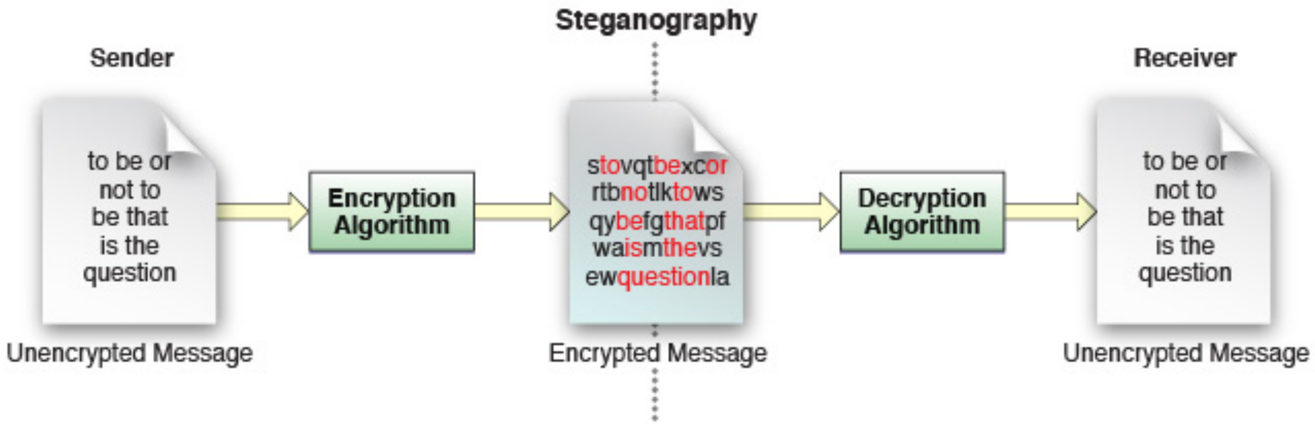


Asymmetric encryption is often used for establishing a shared communication channel. Because asymmetric encryption is computationally expensive, the two endpoints often use asymmetric encryption to exchange a symmetric key, and then use a much faster symmetric encryption algorithm for encrypting and decrypting the actual data.

Asymmetric encryption can also be used to establish trust. By encrypting information with your private key, someone else can read that information with your public key and be certain that it was encrypted by you.

Steganography

Steganography means hiding information in less important bits of another piece of information.


Steganography
Sender
Receiver
to be or not to be that is the question
Encryption Algorithm
stovqtbexcor rtbnotlktows qybefgthatpf waismthevs ewquestionla
Decryption Algorithm
to be or not to be that is the question
Unencrypted Message
Encrypted Message
Unencrypted Message

Steganography is commonly used for storing copyright information into photographs in such a way that is largely indistinguishable from noise unless you know how to look for it.

Steganography can also be used for storing encrypted volumes underneath other encrypted or unencrypted volumes (either by using the unused blocks or by taking advantage of error correction in subtle ways).

Hashing

A hash value, or hash, is a small piece of data derived from a larger piece of data that can serve as a proxy for that larger piece of data. In cryptography, hashes are used when verifying the authenticity of a piece of data. Cryptographic hashing algorithms are essentially a form of (extremely) lossy data compression, but they are specifically designed so that two similar pieces of data are unlikely to hash to the same value.

For example, two schoolchildren frequently passed notes back and forth while deciding when to walk home together. One day, a bully intercepted the note and arranged for Bob to arrive ten minutes early so that he could steal Bob's lunch money. To ensure that their messages were not modified in the future, they devised a scheme in which they computed the remainder after dividing the number of letters in the message by the sum of their ages, then wrote that many dots in the corner of the message. By counting the number of letters, they could (crudely) detect certain modifications to each other's messages.

This is, of course, a contrived example. A simple remainder is a *very* weak hashing algorithm. With good hashing algorithms, collisions are unlikely if you make small changes to a piece of data. This tamper-resistant nature of good hashes makes them a key component in code signing, message signing, and various other tamper detection schemes.

At a high level, hashing is also similar to checksumming (a technique for detecting and correcting errors in transmitted data). However, the goals of these techniques are very different, so the algorithms used are also very different. Checksums are usually designed to allow detection and repair of a single change or a small number of changes. By contrast, cryptographic hashes must reliably detect a large number of changes to a single piece of data but need not tell you how the data changed.

For example, the following command in the shell demonstrates a common hashing algorithm:

```
$ echo "This is a test.  This is only a test." | sha1sum
```

```
7679a5fb1320e69f4550c84560fc6ef10ace4550  -
```

OS X provides a number of C language APIs for performing hashing. These are described further in the documents cited at the end of this chapter.

Signing and Verifying

A signature is a way to prove the authenticity of a message, or to verify the identity of a server, user, or other entity.

In olden days, people sometimes stamped envelopes with a wax seal. This seal not only proved who sent the message but also proved that no one had opened the message and potentially modified it while in transit.

Modern signing achieves many of the same benefits through mathematics. In addition to the data itself, signing and verifying require two pieces of information: the appropriate half of a public-private key pair and a digital certificate.

The sender computes a hash of the message and encrypts it with the private key. The recipient also computes a hash and then uses the corresponding public key to decrypt the sender's hash and compares the hashes. If they are the same, the data was not modified in transit, and you can safely trust that the data was sent by the owner of that key.

The sender's digital certificate is a collection of data that contains a public key and other identifying information, at the sender's discretion, such as a person's name, a company name, a domain name, and a postal address. The purpose of the certificate is to tie a public key to a particular person. If you trust the certificate, you also trust that messages signed by the sender's private key were sent by that person.

To provide a means of determining the legitimacy of a certificate, the sender's certificate is signed by someone else, whose certificate is in turn signed by someone else, and so on, forming a chain of trust to a certificate that the recipient inherently trusts, called an *anchor certificate*. This certificate may be a root certificate—a self-signed certificate that represents a known certificate authority and thus the root of the tree of certificates originating from that authority—or it may be any arbitrary certificate that the user or application developer has explicitly designated as a trusted anchor.

Because the recipient trusts the anchor certificate, the recipient knows that the certificate is valid and, thus, that the sender is who he or she claims to be. The degree to which the recipient trusts a certificate is defined by two factors:

- Each certificate can contain one or more *certificate extensions* that describe how the certificate can be used. For example, a certificate that is trusted for signing email messages might not be trusted for signing executable code.
- The *trust policy* allows you to trust certificates that would otherwise be untrusted and vice versa.

A certificate can also be used for authentication. By signing a nonce (a randomly generated challenge string created specifically for this purpose), a user or server can prove that he, she, or it is in possession of the private key associated with that certificate. If that certificate is considered trusted (by evaluating its chain of trust), then the certificate and signed nonce prove that the user or server must be who he, she, or it claims to be.

Secure Storage

OS X and iOS provide a number of technologies for secure storage. Of these, the three most commonly used technologies are keychains, FileVault, and data protection.

Keychains

In concept, a keychain is similar to a physical key ring in that it is a place where keys and other similarly small pieces of data can be stored for later use in performing cryptographic tasks, but the similarity ends there. With a physical key ring, the owner can take the key and use it to unlock something. With a keychain, apps usually do not access the actual key data itself, so they do not risk exposing the keys even if compromised. Instead, they use a unique identifier to identify those keys, and the actual encryption is performed in a separate process called the Security Server (described later in this document).

Thus, a keychain is in some ways more like a heavily armed security guard in full body armor who carries a key ring. You can ask that guard to unlock a door for you if you are authorized to enter, but you usually can't unlock the door yourself.

OS X also includes a utility that allows users to store and read the data in the keychain, called *Keychain Access*. This utility is described in more detail later, in Keychain Access.

FileVault

In OS X, FileVault uses encryption to provide encrypted storage for the user's files. When FileVault is enabled, the disk is decrypted only after an authorized user logs in. (Note that prior to OS X v10.7, FileVault protected only a user's home directory.)

FileVault and its configuration UI are described in more detail later, in End-User Security Features.

Data Protection

iOS provides APIs that allow an app to make files accessible only while the device is unlocked to protect their contents from prying eyes. With data protection, files are stored in encrypted form and are decrypted only after the user enters his or her passcode.

For apps that run in the background, there are also settings that allow the file to remain available until the user shuts down the device.

To Learn More

For a more detailed conceptual overview of authentication and authorization in OS X, read *Cryptographic Services Guide*.

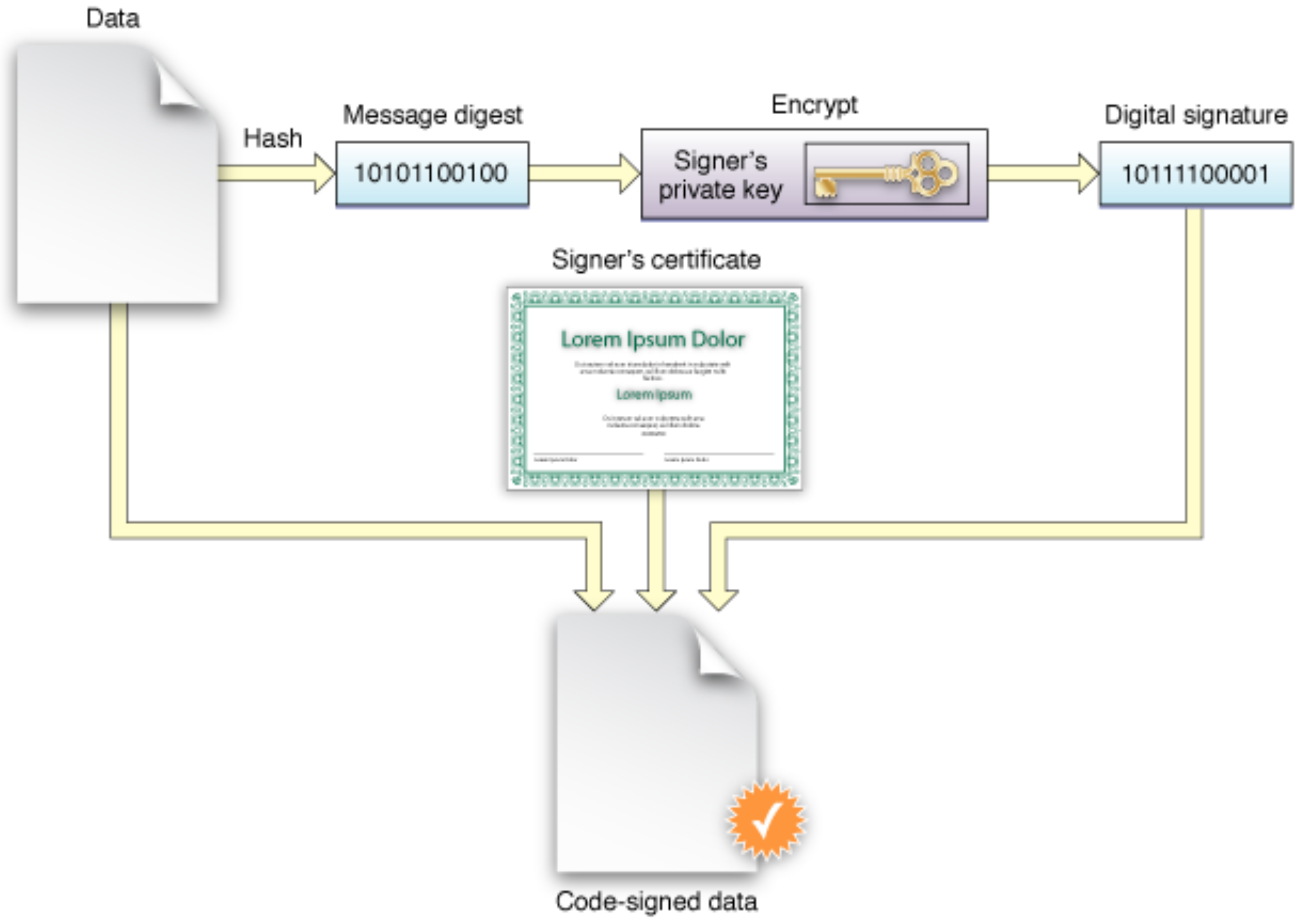
To learn more about creating signing certificates, read Creating Your Signing Certificates in *App Distribution Guide*.

You can also learn about other Apple and third-party security books in Other Security Resources.

Exhibit 20

About Code Signing

Code signing is a security technology, used in OS X, that allows you to certify that an app was created by you. Once an app is signed, the system can detect any change to the app—whether the change is introduced accidentally or by malicious code.



Users appreciate code signing. After installing a new version of a code-signed app, a user is not bothered with alerts asking again for permission to access the keychain or similar resources. As long as the new version uses the same digital signature, OS X can treat the new app exactly as it treated the previous one.

Other OS X security features, such as App Sandbox and parental controls, also depend on code signing.

In most cases, you can rely on Xcode's automatic code signing (described in *App Distribution Guide*), which requires only that you specify a code signing identity in the build settings for your project. This document is for readers who must go beyond automatic code signing—perhaps to troubleshoot an unusual problem, or to incorporate the `codesign(1)` tool into a build system.

At a Glance

The elements of code signing include code signatures, code signing identities, code signing certificates, and security trust policies. Be sure to understand these concepts if you need to perform code signing outside of Xcode.

Relevant chapter: Code Signing Overview

Before you can sign code, you must obtain or create a code signing identity. You then sign your code and prepare it for distribution.

Relevant chapter: Code Signing Tasks

To specify recommended criteria for verifiers to use when evaluating your app's code signature, you use a requirements language specific to the `codesign(1)` and `csreq(1)` commands. You then save your criteria to a binary file as part of your Xcode project.

Relevant chapter: Code Signing Requirement Language

Prerequisites

Read *Security Overview* to understand the place of code signing in the OS X security picture.

See Also

For descriptions of the command-line tools for performing code signing, see the `codesign(1)` and `csreq(1)` man pages.

Exhibit 21

Code Signing Overview

Code signing is a security technique that can be used to ensure code integrity, to determine who developed a piece of code, and to determine the purposes for which a developer intended a piece of code to be used. Although the code signing system performs policy checks based on a code signature, it is up to the caller to make policy decisions based on the results of those checks. When it is the operating system that makes the policy checks, whether your code will be allowed to run in a given situation depends on whether you signed the code and on the requirements you included in the signature.

This chapter describes the benefits of signing code and introduces some of the basic concepts you need to understand in order to carry out the code signing process.

Before you read this chapter, you should be familiar with the concepts described in *Security Overview*.

The Benefits Of Signing Code

When a piece of code has been signed, it is possible to determine reliably whether the code has been modified by someone other than the signer. The system can detect such alteration whether it was intentional (by a malicious attacker, for example) or accidental (as when a file gets corrupted). In addition, through signing, a developer can state that an app update is valid and should be considered by the system as the same app as the previous version.

For example, suppose a user grants the SurfWriter app permission to access a keychain item. Each time SurfWriter attempts to access that item, the system must determine whether it is indeed the same app requesting access. If the app is signed, the system can identify the app with certainty. If the developer updates the app and signs the new version with the same unique identifier, the system recognizes the update as the same app and gives it access without requesting verification from the user. On the other hand, if SurfWriter is corrupted or hacked, the signature no longer matches the previous signature; the system detects the change and refuses access to the keychain item.

Similarly, if you use Parental Controls to prevent your child from running a specific game, and that game has been signed by its manufacturer, your child cannot circumvent the control by renaming or moving files. Parental Controls uses the signature to unambiguously identify the game regardless of its name, location, or version number.

All sorts of code can be signed, including tools, applications, scripts, libraries, plug-ins, and other “code-like” data.

Code signing has three distinct purposes. It can be used to:

- ensure that a piece of code has not been altered
- identify code as coming from a specific source (a developer or signer)
- determine whether code is trustworthy for a specific purpose (for example, to access a keychain item).

To enable signed code to fulfill these purposes, a code signature consists of three parts:

- A seal, which is a collection of checksums or hashes of the various parts of the code, such as the identifier, the `Info.plist`, the main executable, the resource files, and so on. The seal can be used to detect alterations to the code and to the app identifier.
- A digital signature, which signs the seal to guarantee its integrity. The signature includes information that can be used to determine who signed the code and whether the signature is valid.
- A unique identifier, which can be used to identify the code or to determine to which groups or categories the code belongs. This identifier can be derived from the contents of the `Info.plist` for the app, or can be provided explicitly by the signer.

For more discussion of digital signatures, see the following section, Digital Signatures and Signed Code.

To learn more about how a code signature is used to determine the signed code's trustworthiness for a specific purpose, see Code Requirements.

Note that code signing deals primarily with running code. Although it can be used to ensure the integrity of stored code (on disk, for example), that's a secondary use.

To fully appreciate the uses of code signing, you should be aware of some things that signing *cannot* do:

- It can't guarantee that a piece of code is free of security vulnerabilities.
- It can't guarantee that an app will not load unsafe or altered code—such as untrusted plug-ins—during execution.
- It is not a digital rights management (DRM) or copy protection technology. Although the system could determine that a copy of your app had not been properly signed by you, or that its copy protection had been hacked, thus making the signature invalid, there is nothing to prevent a user from running the app anyway.

Digital Signatures and Signed Code

As explained in *Security Overview*, a digital signature uses public key cryptography to ensure data integrity. Like a signature written with ink on paper, a digital signature can be used to identify and authenticate the signer. However, a digital signature is more difficult to forge, and goes one step further: it can ensure that the signed data has not been altered. This is somewhat like designing a paper check or money order in such a way that if someone alters the written amount of money, a watermark with the text "Invalid" becomes visible on the paper.

To create a digital signature, the signing software computes a special type of checksum called a hash (or digest) based on a piece of data or code and encrypts that hash with the signer's private key. This encrypted hash is called a signature.

To verify that signature, the verifying software computes a hash of the data or code. It then uses the signer's public key to decrypt the signature, thus obtaining the original hash as computed by the signer. If the two hashes match, the data has not been modified since it was signed by someone in possession of the signer's private key.

Signed code contains several digital signatures:

- If the code is universal, the object code for each slice (architecture) is signed separately. This signature is stored within the binary file itself.

- Various components of the application bundle (such as the `Info.plist` file, if there is one) are also signed. These signatures are stored in a file called `_CodeSignature/CodeResources` within the bundle.

Code Requirements

It is up to the system or program that is launching or loading signed code to decide whether to verify the signature and, if it does, to determine how to evaluate the results of that verification. The criteria used to evaluate a code signature are called *code requirements*. The signer can specify requirements when signing the code; such requirements are referred to as *internal requirements*. A verifier can read any internal requirements before deciding how to treat signed code. However, it is up to the verifier to decide what requirements to use. For example, Safari could require a plug-in to be signed by Apple in order to be loaded, regardless of whether that plug-in's signature included internal requirements.

One major purpose of code signatures is to allow the verifier to identify the code (such as a program, plug-in, or script) to determine whether it is the same code the verifier has seen before. The criteria used to make this determination are referred to as the code's *designated requirement*. For example, the designated requirement for Apple Mail might be "was signed by Apple and the identifier is `com.apple.Mail`".

To see how this works in practice, assume the user has granted permission to the Apple Mail application to access a keychain item. The keychain uses Mail's designated requirement to identify it: the keychain records the identifier (`com.apple.Mail`) and the signer of the application (Apple) to identify the program allowed to access the keychain item. Whenever Mail attempts to access this keychain item, the keychain looks at Mail's signature to make sure that the program has not been corrupted, that the identifier is `com.apple.Mail`, and that the program was signed by Apple. If everything checks out, the keychain gives Mail access to the keychain item. When Apple issues a new version of Mail, the new version includes a signature, signed by Apple, that identifies the application as `com.apple.Mail`. Therefore, when the user installs the new version of Mail and it attempts to access the keychain item, the keychain recognizes the updated version as the same program and does not prompt the user for verification.

Architecturally, a code requirement is a script, written in a dedicated language, that describes conditions (restrictions) the code must satisfy to be acceptable for some purpose. It is up to you whether to specify internal requirements when you sign code.

The program identifier or the entire designated requirement can be specified by the signer, or can be inferred by the `codesign` tool at the time of signing. In the absence of an explicitly specified designated requirement, the `codesign` utility typically builds a designated requirement from the name of the program found in its `Info.plist` file and the chain of signatures securing the code signature.

Note that validation of signed code against a set of requirements is performed only when the system or some other program needs to determine whether it is safe to trust that code. For example, unsigned code injected into an application through a buffer overflow can still execute because it was not part of the application at launch time. Similarly, an app with an invalid code identifier may still run (depending on policy), but does not get automatic access to keychain items created by previous versions of the app.

The Role of Trust in Code Signing

Trust is determined by policy. A security trust policy determines whether a particular identity should be accepted for allowing something, such as access to a resource or service. Various parts of OS X have different policies, and make this determination differently. For example, a specialized client application might include a set of root certificates that it trusts when communicating with a specific set of servers. However, these root certificates would not be trusted if those same servers were accessed using a web browser.

In much the same way, many parts of OS X (the OS X keychain and parental controls, for example) do not care what entity signed an application; they care only whether the signer has changed since the last time the signature was checked. They use the code signature's designated requirement for this purpose.

Other parts of OS X constrain acceptable signatures to only those drawn from certificate authorities (root certificates) that are trusted anchors on the system performing the validation. For those checks, the nature of the identity used matters. The Application Firewall is one example of this type of policy. Self-signed identities and self-created certificate authorities do not work for these purposes unless the user has explicitly told the operating system to trust the certificates.

You can modify the code signing polices of OS X with the `spctl(8)` command.

Exhibit 22

Code Signing Tasks

This chapter gives procedures and examples for the code signing process. It covers what you need to do before you begin to sign code, how to sign code, and how to ship the code you signed.

Obtaining a Signing Identity

To sign code, you need a code signing identity, which is a private key plus a digital certificate. The digital certificate must have a usage extension that enables it to be used for signing and it must contain the public key that corresponds to the private key. You can use more than one signing identity, each for its own purpose, such as one to be used for beta seeds and one for final, released products. However, most organizations use only one identity.

You can obtain two types of certificates from Apple using the developer portal: Developer ID certificates (for public distribution) and distribution certificates (for submitting to the Mac App Store). To learn more about this, read *Tools Workflow Guide for Mac*.

> **Note:** Apple uses the industry-standard form and format of code signing certificates. Therefore, if your company already has a third-party signing identity that you use to sign code on other systems, you can use it with the OS X `codesign` command. Similarly, if your company is a certificate issuing authority, contact your IT department to find out how to get a signing certificate issued by your company.

If you do not have an existing identity, you should first create one using the Certificate Assistant, which is provided as part of the Keychain Access application. This tool creates a public key, puts it into your keychain, and optionally can produce a certificate signing request that you can then send to Apple (or another certificate authority). The certificate authority then sends you a certificate that, in combination with your private key, completes your digital identity.

▶ **To import a signing certificate with Keychain Access**

> **Note:** If the original private key is not already in your keychain (for example, if you are moving from one development machine to another), you must also import the private key in the same way.

Before you obtain a code signing identity and sign your code, consider the following points:

- Do not ship applications signed by self-signed certificates. A self-signed certificate created with the Certificate Assistant is not recognized by users' operating systems as a valid certificate for any purpose other than validating the designated requirement of your signed code. Because a self-signed certificate has not been signed by a recognized root certificate authority, the user can only verify that two versions of your application came from the same source; they cannot verify that your company is the true source of the code. For more information about root authorities, see Security Concepts.

- Depending on your company's internal policies, you might have to involve your company's Build and Integration, Legal, and Marketing departments in decisions about what sort of signing identity to use and how to obtain it. You should start this process well in advance of the time you need to actually sign the code for distribution to customers.
- Any signed version of your code that gets into the hands of users will appear to have been endorsed by your company for use. Therefore, you might not want to use your "final" signing identity to sign code that is still in development.
- A signing identity, no matter how obtained, is completely compromised if it is ever out of the physical control of whoever is authorized to sign the code. That means that the signing identity's private key must never, under any circumstances, be given to end users, and should be restricted to one or a small number of trusted persons within your company. Before obtaining a signing identity and proceeding to sign code, you must determine who within your company will possess the identity, who can use it, and how it will be kept safe. For example, if the identity must be used by more than one person, you can keep it in the keychain of a secure computer and give the password of the keychain only to authorized users, or you can put the identity on a smart card to which only authorized users have the PIN.
- A self-signed certificate created by the Certificate Assistant is adequate for internal testing and development, regardless of what procedures you put in place to sign released products.

▶ **To use the Certificate Assistant to create a self-signed signing identity**

Adding an Info.plist to Single-File Tools

As discussed in Code Requirements, the system often uses the `Info.plist` file of an application bundle to determine the code's designated requirement. Although single-file tools don't normally have an `Info.plist`, you can add one. To do so, use the following procedure:

1. Add an `Info.plist` file to your project (including adding it to your source control).
2. Make sure the `Info.plist` file has the following keys:
   - `CFBundleIdentifier`
   - `CFBundleName`
3. The value for `CFBundleIdentifier` is used as the default unique name of your program for Code Signing purposes. Because the `CFBundleIdentifier` value is also used when your application accesses resources in the application bundle, it may sometimes be necessary to use a non-unique `CFBundleIdentifier` value for a helper. If you do this, you must provide a different, unique identifier for code signing purposes by passing the `-i` or `--identifier` flag to the `codesign` command.

   The identifier used for signing must be globally unique. To ensure uniqueness, you should include your company’s name in the value. The usual form for this identifier is a hierarchical name in reverse DNS notation, starting with the top level domain, followed by the company name, followed by the organization within the company, and ending with the product name. For example, the `CFBundleIdentifier` value for the `codesign` command is `com.apple.security.codesign`.

4. The value for `CFBundleName` shows up in system dialogs as the name of your program, so it should match your marketing name for the product.
5. Add the following arguments to your linker flags:

   `-sectcreate __TEXT __info_plist` *Info.plist_path*

   where *Info.plist_path* is the complete path of the `Info.plist` file in your project.

   In Xcode, for example, you would add these linker flags to the `OTHER_LDFLAGS` build variable (Other Linker Flags in the target’s build rules).

For example, here are the contents of the `Info.plist` file for the `codesign` command:

```
<plist version="1.0">
<dict>
    <key>CFBundleDevelopmentRegion</key>
    <string>English</string>
    <key>CFBundleIdentifier</key>
    <string>com.apple.security.codesign</string>
    <key>CFBundleInfoDictionaryVersion</key>
    <string>6.0</string>
    <key>CFBundleName</key>
    <string>codesign</string>
    <key>CFBundleVersion</key>
    <string>0.3</string>
</dict>
</plist>
```

Signing Your Code

You use the `codesign` command to sign your code. This section discusses what to sign and gives some examples of the use of `codesign`. See the `codesign(1)` manual page for a complete description of its use.

What to Sign

You should sign every executable in your product, including applications, tools, hidden helper tools, utilities and so forth. Signing an application bundle covers its resources, but not its subcomponents such as tools and sub-bundles. Each of these must be signed independently.

If your application consists of a big UI part with one or more little helper tools that try to present a single face to the user, you can make them indistinguishable to code signing by giving them all the exact same code signing identifier. (You can do that by making sure that they all have the same `CFBundleIdentifier` value in their `Info.plist`, or by using the `-i` option in the `codesign` command, to assign the same identifier.) In that case, all your program components have access to the same keychain items and validate as the same program. Do this only if the programs involved are truly meant to form a single entity, with no distinctions made.

A universal binary (bundle or tool) automatically has individual signatures applied to each architecture component. These are independent, and usually only the native architecture on the end user's system is verified.

In the case of installer packages (.pkg and .mpkg bundles), everything is implicitly signed: The CPIO archive containing the payload, the CPIO archive containing install scripts, and the bill of materials (BOM) each have a hash recorded in the XAR header, and that header in turn is signed. Therefore, if you modify an install script (for example) after the package has been signed, the signature will be invalid.

You may also want to sign your plug-ins and libraries. Although this is not currently required, it will be in the future, and there is no disadvantage to having signatures on these components.

Important: When code signing a framework, you must sign a particular *version* of the framework, not the framework as a whole. For example:

```
codesign -s my-signing-identity ../MyCustomFramework/Versions/A
```

Depending on the situation, `codesign` may add to your Mach-O executable file, add extended attributes to it, or create new files in your bundle's Contents directory. None of your other files is modified.

When to Sign

You can run `codesign` at any time on any system running OS X v10.5 or later, provided you have access to the signing identity. You can run it from a shell script phase in Xcode if you like, or as a step in your Makefile scripts, or anywhere else you find suitable. Signing is typically done as part of the product mastering process, after quality assurance work has been done. Avoid signing pre-final copies of your product so that no one can mistake a leaked or accidentally released incomplete version of your product for the real thing.

Your final signing must be done after you are done building your product, including any post-processing and assembly of bundle resources. Code signing detects any change to your program after signing, so if you make any changes at all after signing, your code will be rejected when an attempt is made to verify it. Sign your code before you package the product for delivery.

Because each architecture component is signed independently, it is all right to perform universal-binary operations (such as running the `lipo` command) on signed programs. The result will still be validly signed as long as you make no other changes.

Using the codesign Command

The codesign command is fully described in the codesign(1) manual page. This section provides some examples of common uses of the command. Note that your signing identity must be in a keychain for these commands to work.

Signing Code

To sign the code located at <code-path>, using the signing identity <identity>, use the following command:

```
codesign -s <identity> <code-path> …
```

The <code-path> value may be a bundle folder or a specific code binary. See What to Sign for more details.

The identity can be named with any (case sensitive) substring of the certificate's common name attribute, as long as the substring is unique throughout your keychains. (Signing identities are discussed in Obtaining a Signing Identity.)

As is typical of Unix-style commands, this command gives no confirmation of success. To get some feedback, include the -v option:

```
codesign -s <identity> -v <code-path> …
```

Use the -r option to specify an internal requirement. With this option you can specify a text file containing the requirements, a precompiled requirements binary, or the actual requirement text prefixed with an equal sign (=). For example, to add an internal requirement that all libraries be signed by Apple, you could use the following option:

```
-r="library => anchor apple"
```

The code requirement language is described in Code Signing Requirement Language.

If you have built your own certificate hierarchy (perhaps using Certificate Assistant—see Obtaining a Signing Identity), and want to use your certificate's anchor to form a designated requirement for your program, you could use the following command:

```
codesign -s signing-identity -r="designated => anchor /my/anchor/cert and identifier
com.mycorp.myprog"
```

Note that the requirement source language accepts either an SHA1 hash of a certificate (for example H"abcd....") or a path to the DER encoded certificate in a file. It does not currently accept a reference to the certificate in a keychain, so you have to export the certificate before executing this command.

You can also use the csreq command to write the requirements out to a file, and then use the path to that file as the input value for the -r option in the codesign command. See the manual page for csreq(1) for more information on that command.

Here are some other samples of requirements:

- `anchor apple` –the code is signed by Apple
- `anchor trusted` –the anchor is trusted (for code signing) by the system
- `certificate leaf = /path/to/certificate` –the leaf (signing) certificate is the one specified
- `certificate leaf = /path/to/certificate and identifier "com.mycorp.myprog"` –the leaf certificate and program identifier are as specified
- `info[mykey] = myvalue` – the `Info.plist` key `mykey` exists and has the value `myvalue`

Except for the explicit `anchor trusted` requirement, the system does not consult its trust settings database when verifying a code requirement. Therefore, as long as you don't add this designated requirement to your code signature, the anchor certificate you use for signing your code does not have to be introduced to the user's system for validation to succeed.

Adding Entitlements for Sandboxing

If you want to enable App Sandbox for an application, you must add an entitlement property list during the signing process. To do this, add the `--entitlements` flag and an appropriate property list. For example:

```
codesign --entitlements /path/to/entitlements.plist -s <identity> <code-path> …
```

For a list of entitlement keys that can appear in the entitlement property list, see *Entitlement Key Reference*.

Verifying Code

To verify the signature on a signed binary, use the `-v` option with no other options:

```
codesign -v <code-path> …
```

This checks that the code binaries at `<code-path>` are actually signed, that the signature is valid, that all the sealed components are unaltered, and that the whole thing passes some basic consistency checks. It does not by default check that the code satisfies any requirements except its own designated requirement. To check a particular requirement, use the `-R` option. For example, to check that the Apple Mail application is identified as Mail, signed by Apple, and secured with Apple's root signing certificate, you could use the following command:

```
codesign -v -R="identifier com.apple.mail and anchor apple" /Applications/Mail.app
```

Note that, unlike the `-r` option, the `-R` option takes only a single requirement rather than a requirements collection (no `=>` tags). Add one or more additional `-v` options to get details on the validation process.

If you pass a number rather than a path to the verify option, `codesign` takes the number to be the process ID (pid) of a running process, and performs dynamic validation instead.

Getting Information About Code Signatures

To get information about a code signature, use the `-d` option. For example, to output the code signature's internal requirements to standard out, use the following command:

```
codesign -d -r code-path
```

Note that this option does not verify the signature.

Using the spctl Tool to Test Code Signing

The `spctl(8)` tool can be used to test your code signatures against various system policies that the user may set. The basic syntax for code signing assessment is shown below:

```
# Assess an application or tool
spctl --assess --type execute myTool


# Assess an installer package
spctl --assess --type install myInstallerPackage.pkg
```

If your application or package signature is valid, these tools exit silently with an exit status of `0`. (Type `echo $?` to display the exit status of the last command.) If the signature is invalid, these tools print an error message and exit with a nonzero exit status.

For more detailed information about why the assessment failed, you can add the `--verbose` flag. For example:

```
spctl --assess --verbose=4 /bin/ls
```

This prints the following output:

```
    /bin/ls: accepted

    source=Apple System
```

To see *everything* the system has to say about an assessment, pass the `--raw` option. With this flag, the `spctl` tool prints a detailed assessment as a property list.

To whitelist a program (exactly as if the UI did it), type:

```
spctl --add --label mytest /some/program
```

The --label is an optional tag that you can add to your own rules. This tag allows you to remove the rule easily by typing:

```
spctl --remove --label mytest
```

Note that this removes all rules that match the label, which means that it is a handy way to clean up after testing. You can also temporarily suspend your rules by typing:

```
spctl --disable --label mytest
```

and reenable them later by typing:

```
spctl --enable --label mytest
```

To see a list of the current assessment rules, use the `--list` flag. For example:

```
spctl --list --type execute
```

The resulting list of rules might look like this:

```
    3[Apple System] P0 allow execute

        anchor apple

    4[Mac App Store] P0 allow execute

        anchor apple generic and certificate leaf[field.1.2.840.113635.100.6.1.9]
exists

    5[Developer ID] P0 allow execute

        anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] exists
and certificate leaf[field.1.2.840.113635.100.6.1.13] exists

    7[UNLABELED] P0 allow execute [/var/tmp/firefly/RUN-FIREFLY-JOBS/test1.app]

        cdhash H"f34c03450da53c07ac69282089b68723327f278a"

    8[UNLABELED] P0 allow execute [/var/tmp/firefly/RUN-FIREFLY-JOBS/test1.app]

        identifier "org.tpatko.Run-Firefly-Job-X-Cores" and certificate root =
H"5056a3983e3b7f44e17e3db8e483b35b6745b236"
```

Notice that the list above includes a number of predefined rules that describe the handling of certain classes of code. For example, rule 5 captures all applications signed by a Developer ID. You can disable those applications by typing:

```
spctl --disable --label "Developer ID"
```

This command tells the system to no longer allow execution of any Developer ID-signed applications that the user has not previously run. This is exactly what happens when you use the preference UI to switch to "Mac App Store only".

Each rule in the list has a unique number that can be used to address it. For example, if you type:

```
spctl --list --label "Developer ID"
```

you might get a list of rules that looks like this:

```
    5[Developer ID] P0 allow execute

        anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] exists
and certificate leaf[field.1.2.840.113635.100.6.1.13] exists

    6[Developer ID] P0 allow install

        anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] exists
and certificate leaf[field.1.2.840.113635.100.6.1.14] exists
```

Notice that there are separate rules for execution (5) and installation (6), and you can enable and disable them separately. For example, to enable installation of new applications signed with a Developer ID, you can type:

```
spctl --enable --rule 6
```

Finally, `spctl` allows you to enable or disable the security assessment policy subsystem. By default, assessment is turned off, which means that missing or invalid code signatures do not prevent an application from launching. However, it is strongly recommended that you test your application with assessment enabled to ensure that your application works correctly.

To enable or disable assessment, issue one of the following commands.

```
sudo spctl --master-enable   # enables assessment

sudo spctl --master-disable  # disables assessment

spctl --status               # shows whether assessment is enabled
```

For more information, see the manual page for `spctl(8)`.

Shipping and Updating Your Product

The only thing that matters to the code signing system is that the signed code installed on the user's system identical to the code that you signed. It does not matter how you package, deliver, or install your product as long as you don't introduce any changes into the product. Compression, encoding, encrypting, and even binary patching the code are all right as long as you end up with exactly what you started with. You can use any installer you like, as long as it doesn't write anything into the product as it installs it. Drag-installs are fine as well.

When you have qualified a new version of your product, sign it just as you signed the previous version, with the same identifier and the same designated requirement. The user's system will consider the new version of your product to be the same program as the previous version. In particular, the keychain will not distinguish older and newer versions of your program as long as both were signed and the unique Identifier hasn't changed.

You can take a partial-update approach to revising your code on the user's system. To do so, sign the new version as usual, then calculate the differences between the new and the old signed versions, and transmit the differences. Because the differences include the new signature data, the result of installing the changes on the end-user's system will be the newly signed version. You cannot patch a signed application in the field. If you do so, the system will notice that the application has changed and will invalidate the signature, and there is no way to re-validate or resign the application in the field.

Exhibit 23

Code Signing Requirement Language

When you use the `codesign` command to sign a block of code, you can specify internal requirements; that is, the criteria that you recommend should be used to evaluate the code signature. It is up to the verifier to decide whether to apply the internal requirements or some other set of requirements when deciding how to treat the signed code. You use the code requirement language described in this chapter when specifying requirements to the `codesign` or `csreq` command (see the manual pages for `codesign(1)` and `csreq(1)`).

This chapter describes the requirement language source code. You can compile a set of requirements and save them in binary form using the `csreq` command. You can provide requirements to the `codesign` command either as source code or as a binary file. Both the `codesign` and `csreq` commands can convert a binary requirement set to text. Although there is some flexibility in the source code syntax (for example, quotes can always be used around string constants but are not always required), conversion from binary to text always uses the same form:

- Parentheses are placed (usually only) where required to clarify operator precedence.
- String constants are quoted (usually only) where needed.
- Whether originally specified as constants or through file paths, certificate hashes are always returned as hash constants.
- Comments in the original source are not preserved in the reconstructed text.

Language Syntax

Some basic features of the language syntax are:

- Expressions use conventional infix notation (that is, the operator is placed between the two entities being acted on; for example *quantity* < *constant*).
- Keywords are reserved, but can be quoted to be included as part of ordinary strings.
- Comments are allowed in C, Objective C, and C++.
- Unquoted whitespace is allowed between tokens, but strings containing whitespace must be quoted.
- Line endings have no special meaning and are treated as whitespace.

Evaluation of Requirements

A requirement constitutes an expression without side effects. Each requirement can have any number of subexpressions, each of which is evaluated with a Boolean (succeed-fail) result. There is no defined order of evaluation. The subexpressions are combined using logical operators in the expression to yield an overall Boolean result for the expression. Depending on the operators used, an expression can succeed even if some subexpressions fail. For example, the expression

```
anchor apple or anchor = "/var/db/yourcorporateanchor.cert"
```

succeeds if either subexpression succeeds—that is, if the code was signed either by Apple or by your company—even though one of the subexpressions is sure to fail.

If an error occurs during evaluation, on the other hand, evaluation stops immediately and the `codesign` or `csreq` command returns with a result code indicating the reason for failure.

Constants

This section describes the use of string, integer, hash-value, and binary constants in the code signing requirement language.

String Constants

String constants must be enclosed by double quotes (`" "`) unless the string contains only letters, digits, and periods (.), in which case the quotes are optional. Absolute file paths, which start with a slash, do not require quotes unless they contain spaces. For example:

```
com.apple.mail                      //no quotes are required
"com.apple.mail"                    //quotes are optional
"My Company's signing identity"     //requires quotes for spaces and apostrophe
/Volumes/myCA/root.crt              //no quotes are required
"/Volumes/my CA/root.crt"           //space requires quotes
"/Volumes/my_CA/root.crt"           //underscore requires quotes
```

It’s never incorrect to enclose the string in quotes—if in doubt, use quotes.

Use a backslash to “escape” any character. For example:

```
"one \" embedded quote"             //one " embedded quote
"one \\ embedded backslash"         //one \ embedded backslash
```

There is nothing special about the single quote character (').

Integer Constants

Integer constants are written as decimal constants are in C. The language does not allow radix prefixes (such as `0x`) or leading plus or minus (`+` or `-`) signs.

Hash Constants

Hash values are written either as a hexadecimal number in quotes preceded by an `H`, or as a path to a file containing a binary certificate. If you use the first form, the number must include the exact number of digits in the hash value. A SHA-1 hash (the only kind currently supported) requires exactly 40 digits; for example:

```
H"0123456789ABCDEFFEDCBA98765432100A2BC5DA"
```

You can use either uppercase or lowercase letters (`A..F` or `a..f`) in the hexadecimal numbers.

If you specify a file path, the compiler reads the binary certificate and calculates the hash for you. The compiled version of the requirement code includes only the hash; the certificate file and the path are not retained. If you convert the requirement back to text, you get the hexadecimal hash constant. The file path must point to a file containing an X.509 DER encoded certificate. No container forms (PKCS7, PKCS12) are allowed, nor is the OpenSSL "PEM" form supported.

Variables

There are currently no variables in the requirement language.

Logical Operators

The requirement language includes the following logical operators, in order of decreasing precedence:

- `!` (negation)
- `and` (logical AND)
- `or` (logical OR)

These operators can be used to combine subexpressions into more complex expressions. The negation operator (`!`) is a unary prefix operator. The others are infix operators. Parentheses can be used to override the precedence of the operators.

Because the language is free of side effects, evaluation order of subexpressions is unspecified.

Comparison Operations

The requirement language includes the following comparison operators:

- `=` (equals)
- `<` (less than)
- `>` (greater than)

- `<=` (less than or equal to)
- `>=` (greater than or equal to)
- `exists` (value is present)

The value-present (`exists`) operator is a unary suffix operator. The others are infix operators.

There are no operators for non-matches (not equal to, not greater than, and so on). Use the negation operator (`!`) together with the comparison operators to make non-match comparisons.

Equality

All equality operations compare some value to a constant. The value and constant must be of the same type: a string matches a string constant, a data value matches a hexadecimal constant. The equality operation evaluates to `true` if the value exists and is equal to the constant. String matching uses the same matching rules as `CFString` (see *CFString Reference*).

In match expressions (see Info, Part of a Certificate, and Entitlement), substrings of string constants can be matched by using the `*` wildcard character:

- `value = *constant*` is `true` if the value exists and any substring of the value matches the constant; for example:
  - `thunderbolt = *under*`
  - `thunderbolt = *thunder*`
  - `thunderbolt = *bolt*`
- `value = constant*` is `true` if the value exists and begins with the constant; for example:
  - `thunderbolt = thunder*`
  - `thunderbolt = thun*`
- `value = *constant` is `true` if the value exists and ends with the constant; for example:
  - `thunderbolt = *bolt`
  - `thunderbolt = *underbolt`

If the constant is written with quotation marks, the asterisks must be outside the quotes. An asterisk inside the quotation marks is taken literally. For example:

- `"ten thunderbolts" = "ten thunder"*` is `true`
- `"ten thunder*bolts" = "ten thunder*"*` is `true`
- `"ten thunderbolts" = "ten thunder*"` is `false`

Inequality

Inequality operations compare some value to a constant. The value and constant must be of the same type: a string matches a string constant, a data value matches a hexadecimal constant. String comparisons use the same matching rules as `CFString` with the `kCFCompareNumerically` option flag; for example, `"17.4"` is greater than `"7.4"`.

Existence

The existence operator tests whether the value exists. It evaluates to `false` only if the value does not exist at all or is exactly the Boolean value `false`. An empty string and the number `0` are considered to exist.

Constraints

Several keywords in the requirement language are used to require that specific certificates be present or other conditions be met.

Identifier

The expression

`identifier =` *constant*

succeeds if the unique identifier string embedded in the code signature is exactly equal to *constant*. The equal sign is optional in identifier expressions. Signing identifiers can be tested only for exact equality; the wildcard character (`*`) can not be used with the identifier constraint, nor can identifiers be tested for inequality.

Info

The expression

`info [`*key*`]`*match expression*

succeeds if the value associated with the top-level key in the code's `info.plist` file matches *match expression*, where *match expression* can include any of the operators listed in Logical Operators and Comparison Operations. For example:

```
info [CFBundleShortVersionString] < "17.4"
```

or

```
info [MySpecialMarker] exists
```

You must specify *key* as a string constant.

If the value of the specified key is a string, the match is applied to it directly. If the value is an array, it must be an array of strings and the match is made to each in turn, succeeding if any of them matches. Substrings of string constants can be matched by using any match expression (see Comparison Operations).

If the code has no `info.plist` file, or the `info.plist` does not contain the specified key, this expression evaluates to `false` without returning an error.

Certificate

Certificate constraints refer to certificates in the certificate chain used to validate the signature. Most uses of the `certificate` keyword accept an integer that indicates the position of the certificate in the chain: positive integers count from the leaf (0) toward the anchor. Negative integers count backward from the anchor (-1). For example, `certificate 1` is the intermediate certificate that was used to sign the leaf (that is, the signing certificate), and `certificate -2` indicates the certificate that was directly signed by the anchor. Note that this convention is the same as that used for array indexing in the Perl and Ruby programming languages:

Anchor	First intermediate	Second intermediate	Leaf
`certificate 3`	`certificate 2`	`certificate 1`	`certificate 0`
`certificate -1`	`certificate -2`	`certificate -3`	`certificate -4`

Other keywords include:

- `certificate root`—the anchor certificate; same as certificate 0
- `anchor`—same as `certificate root`
- `certificate leaf`—the signing certificate; same as `certificate -1`

Note: The short form `cert` is allowed for the keyword `certificate`.

If there is no certificate at the specified position, the constraint evaluates to `false` without returning an error.

If the code was signed using an ad-hoc signature, there are no certificates at all and all certificate constraints evaluate to `false`. (An ad-hoc signature is created by signing with the pseudo-identity `-` (a dash). An ad-hoc signature does not use or record a cryptographic identity, and thus identifies exactly and only the one program being signed.)

If the code was signed by a self-signed certificate, then the leaf and root refer to the same single certificate.

Whole Certificate

To require a particular certificate to be present in the certificate chain, use the form

`certificate` *position* `=` *hash*

or one of the equivalent forms discussed above, such as `anchor =` *hash*. Hash constants are described in Hash Constants.

For Apple's own code, signed by Apple, you can use the short form

```
anchor apple
```

For code signed by Apple, including code signed using a signing certificate issued by Apple to other developers, use the form

```
anchor apple generic
```

Part of a Certificate

To match a well-defined element of a certificate, use the form

`certificate` *position*`[`*element*`]`*match expression*

where *match expression* can include the `*` wildcard character and any of the operators listed in Logical Operators and Comparison Operations. The currently supported elements are as follows:

Note: Case is significant in element names.

Element name	Meaning	Comments
`subject.CN`	Subject common name	Shown in Keychain Access utility
`subject.C`	Subject country name	
`subject.D`	Subject description	
`subject.L`	Subject locality	
`subject.O`	Subject organization	Usually company or organization
`subject.OU`	Subject organizational unit	
`subject.STREET`	Subject street address	

Certificate field by OID

To check for the existence of any certificate field identified by its X.509 object identifier (OID), use the form

`certificate` *position* `[field.`*OID*`] exists`

The object identifier must be written in numeric form (*x*.*y*.*z*...) and can be the OID of a certificate extension or of a conventional element of a certificate as defined by the CSSM standard (see Chapter 31 in *Common Security: CDSA and CSSM*, version 2 (with corrigenda) by the Open Group (http://www.opengroup.org/security/cdsa.htm)).

Trusted

The expression

`certificate` *position* `trusted`

succeeds if the certificate specified by *position* is marked trusted for the code signing certificate policy in the system's Trust Settings database. The *position* argument is an integer or keyword that indicates the position of the certificate in the chain; see the discussion under Certificate.

The expression

`anchor trusted`

succeeds if any certificate in the signature's certificate chain is marked trusted for the code signing certificate policy in the system's Trust Settings database, provided that no certificate closer to the leaf certificate is explicitly untrusted.

Thus, using the `trusted` keyword with a certificate position checks only the specified certificate, while using it with the `anchor` keyword checks all the certificates, giving precedence to the trust setting found closest to the leaf.

> **Important:** The syntax `anchor trusted` is *not* a synonym for `certificate anchor trusted`. Whereas the former checks all certificates in the signature, the latter checks only the anchor certificate.

Certificates can have per-user trust settings and system-wide trust settings, and trust settings apply to specific policies. The `trusted` keyword in the code signing requirement language causes trust to be checked for the specified certificate or certificates for the user performing the validation. If there are no settings for that user, then the system settings are used. In all cases, only the trust settings for the code-signing policy are checked. Policies and trust are discussed in *Certificate, Key, and Trust Services Programming Guide*.

> **Important:** If you do not include an expression using the `trusted` keyword in your code signing requirement, then the verifier does not check the trust status of the certificates in the code signature at all.

Entitlement

The expression

`entitlement [`*key*`]` *match expression*

succeeds if the value associated with the specified key in the signature's embedded entitlement dictionary matches *match expression*, where *match expression* can include the `*` wildcard character and any of the operators listed in Logical Operators and Comparison Operations. You must specify *key* as a string constant. The entitlement dictionary is included in signatures for certain platforms.

Code Directory Hash

The expression

`cdhash` *hash-constant*

computes a SHA-1 hash of the program's CodeDirectory resource and succeeds if the value of this hash exactly equals the specified hash constant.

The CodeDirectory resource is the master directory of the contents of the program. It consists of a versioned header followed by an array of hashes. This array consists of a set of optional special hashes for other resources, plus a vector of hashes for pages of the main executable. The CodeSignature and CodeDirectory resources together make up the signature of the code.

You can use the codesign utility with (at least) three levels of verbosity to obtain the hash constant of a program's CodeDirectory resource:

```
$ codesign -dvvv /bin/ls
...
CodeDirectory v=20001 size=257 flags=0x0(none) hashes=8+2 location=embedded
CDHash=4bccbc576205de37914a3023cae7e737a0b6a802
...
```

Because the code directory changes whenever the program changes in a nontrivial way, this test can be used to unambiguously identify one specific version of a program. When the operating system signs an otherwise unsigned program (so that the keychain or Parental Controls can recognize the program, for example), it uses this requirement.

Requirement Sets

A requirement set is a collection of distinct requirements, each indexed (tagged) with a type code. The expression

tag `=>` *requirement*

applies *requirement* to the type of code indicated by *tag*, where possible tags are

- `host`—this requirement is applied to the direct host of this code module; each code module in the hosting path can have its own host requirement, where the hosting path is the chain of code signing hosts starting with the most specific code known to be running, and ending with the root of trust (the kernel)
- `guest`—this requirement is applied to each code module that is hosted by this code module
- `library`—this requirement is applied to all libraries mounted by the signed code
- `designated`—this is an explicitly specified designated requirement for the signed code; if there is no explicitly specified designated requirement for the code, then there is no `designated` internal requirement

The primary use of requirement sets is to represent the internal requirements of the signed code. For example:

```
    codesign -r='host => anchor apple and identifier com.apple.perl designated =>
anchor /my/root and identifier com.bar.foo'
```

sets the internal requirements of some code, having a host requirement of `anchor apple and identifier com.apple.perl` (“I'm a Perl script and I want to be run by Apple's Perl interpreter”) and an explicit designated requirement of `anchor /my/root and identifier com.bar.foo`. Note that this command sets no guest or library requirements.

You can also put the requirement set in a file and point to the file:

```
    codesign -r myrequirements.rqset
```

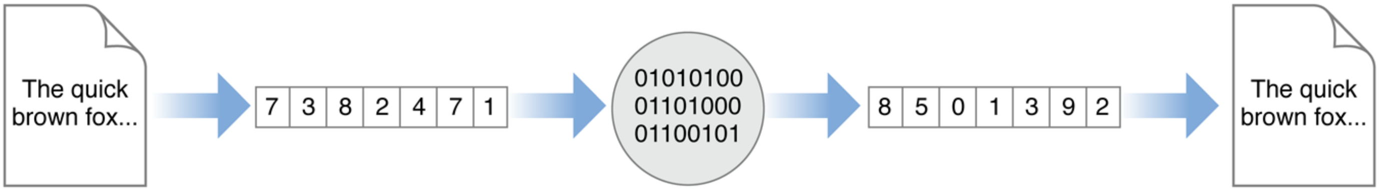
where the file `myrequirements.rqset` might contain:

```
    //internal requirements

      host => anchor apple and identifier com.apple.perl //require Apple's Perl
interpreter

      designated => anchor /my/root and identifier com.bar.foo
```

Exhibit 24

About Cryptographic Services

OS X and iOS provide a number of technologies that provide cryptographic services—encryption and decryption, hashing, random number generation, secure network communication, and so on. These technologies can be used to secure data at rest (when stored on your hard drive or other media), secure data in transit, determine the identity of a third party, and build additional security technologies.



At a Glance

Some of the cryptographic services provided by iOS and OS X include:

- Encryption and decryption (both general-purpose and special-purpose)
- Key management using keychains
- Cryptographically strong random number generation
- Secure communication (SSL and TLS)
- Secure storage using FileVault and iOS File Protection

Encryption, Signing and Verifying, and Digital Certificates Can Protect Data from Prying Eyes

There are two main types of encryption: symmetric encryption, in which a single shared key is used for encrypting and decrypting data, and asymmetric encryption, in which you use one key to encrypt data and a separate (but related) key to decrypt the data. You can use a hash to detect modifications to a piece of data. You can combine hashes with asymmetric keys to create a digital signature that, when verified against a digital certificate, proves the source of a piece of data. Digital certificates, in turn, are verified by verifying the signature of the party that signed the certificate, then verifying that party's certificate, and so on until you reach a certificate that you trust inherently, called an *anchor certificate*.

Relevant Chapter: Cryptography Concepts In Depth

OS X and iOS Provide Encryption and Hashing APIs

OS X and iOS provide a number of APIs for encrypting and hashing data, including Keychain Services;

Cryptographic Message Syntax Services; Certificate, Key, and Trust Services; Common Crypto; and Security Transforms.

Relevant Chapter: Encrypting and Hashing Data

Keychains Help You Store Secret Information

If your app must store encryption keys, passwords, certificates, and other security-related information, it should use a keychain. Keychains provide secure storage for small pieces of information so that is not accessible by other apps running on the system, and so that it is accessible only after the user has logged in or unlocked the device. OS X and iOS provide two APIs for working with the keychain and keys obtained from the keychain: the Certificate, Key, and Trust Services API and the Keychain Services API.

Relevant Chapter: Managing Keys, Certificates, and Passwords

OS X and iOS Provide Cryptographically Secure Random Number Generators

Some cryptographic tasks require you to generate cryptographically strong pseudorandom numbers. OS X can provide these numbers through the `/dev/random` device node. iOS can provide these numbers through the Randomization Services API.

Relevant Chapter: Generating Random Numbers

OS X and iOS Provide Secure Network Communication APIs

Transmitting data securely requires a secure communications channel. OS X and iOS provide a number of APIs for establishing secure communications channels, including the URL Loading System, socket streams in Core Foundation and Foundation, and Secure Transport.

Relevant Chapter: Transmitting Data Securely

Deprecated Technologies

Although the CDSA and CSSM API is deprecated in OS X v10.7 and later, you may still need to use it in a few situations. For this reason, its documentation is provided as an appendix.

Relevant Chapter: CDSA Overview

Prerequisites

Before reading this document, you should be familiar with the concepts in *Security Overview* and *Secure Coding Guide*.

See Also

For more information about OS X authentication and authorization (built on top of encryption technologies), read *Authentication, Authorization, and Permissions Guide*.

Exhibit 25

Cryptography Concepts In Depth

The word cryptography (from Greek *kryptos*, meaning hidden) at its core refers to techniques for making data unreadable to prying eyes. However, cryptography can also be used for other purposes. Cryptography includes a range of techniques that can be used for verifying the authenticity of data (detecting modifications), determining the identity of a person or other entity, determining who sent a particular message or created a particular piece of data, sending data securely across a network, locking files securely behind a password or passphrase, and so on.

This chapter describes a number of these techniques, beginning with basic encryption, then moving on to other cryptographic constructs built on top of it.

> **Note:** This chapter repeats many of the concepts in *Security Overview*, but with additional detail and depth. You may find it helpful to read that document before reading this chapter.

What Is Encryption?

Encryption is the transformation of data into a form in which it cannot be made sense of without the use of some key. Such transformed data is referred to as *ciphertext*. Use of a key to reverse this process and return the data to its original (cleartext or plaintext) form is called *decryption*. Most of the security APIs in OS X and iOS rely to some degree on encryption of text or data. For example, encryption is used in the creation of certificates and digital signatures, in secure storage of secrets in the keychain, and in secure transport of information.

Encryption can be anything from a simple process of substituting one character for another—in which case the key is the substitution rule—to a complex mathematical algorithm. For purposes of security, the more difficult it is to decrypt the ciphertext, the better. On the other hand, if the algorithm is too complex, takes too long to do, or requires keys that are too large to store easily, it becomes impractical for use in a personal computer. Therefore, some balance must be reached between *strength* of the encryption (that is, how difficult it is for someone to discover the algorithm and the key) and ease of use.

For practical purposes, the encryption only needs to be strong enough to protect the data for the amount of time the data might be useful to a person with malicious intent. For example, if you need to keep your bid on a contract secret only until after the contract has been awarded, an encryption method that can be broken in a few weeks will suffice. If you are protecting your credit card number, you probably want an encryption method that cannot be broken for many years.

Types of Encryption

There are two main types of encryption in use in computer security, referred to as *symmetric key encryption* and *asymmetric key encryption*. A closely related process to encryption, in which the data is transformed using a key and a mathematical algorithm that cannot be reversed, is called *cryptographic hashing*. The remainder of this section discusses encryption keys, key exchange mechanisms (including the Diffie-Hellman key exchange used in some secure transport protocols), and cryptographic hash functions.

Symmetric Keys

Symmetric key cryptography (also called *secret key cryptography*) is the classic use of keys that most people are familiar with: The same key is used to encrypt and decrypt the data. The classic, and most easily breakable, version of this is the Caesar cipher (named for Julius Caesar), in which each letter in a message is replaced by a letter that is a fixed number of positions away in the alphabet (for example, “a” is replaced by “c”, “b” is replaced by “d”, and so forth). In the Caesar cipher, the key used to encrypt and decrypt the message is simply the number of places by which the alphabet is rotated and the direction of that rotation. Modern symmetric key algorithms are much more sophisticated and much harder to break. However, they share the property of using the same key for encryption and decryption.

There are many different algorithms used for symmetric key cryptography, offering anything from minimal to nearly unbreakable security. Some of these algorithms offer strong security, easy implementation in code, and rapid encryption and decryption. Such algorithms are very useful for such purposes as encrypting files stored on a computer to protect them in case an unauthorized individual uses the computer. They are somewhat less useful for sending messages from one computer to another, because both ends of the communication channel must possess the key and must keep it secure. Distribution and secure storage of such keys can be difficult and can open security vulnerabilities.

In 1968, the USS *Pueblo*, a U.S. Navy intelligence ship, was captured by the North Koreans. At the time, every Navy ship carried symmetric keys for a variety of code machines at a variety of security levels. Each key was changed daily. Because there was no way to know how many of these keys had not been destroyed by the Pueblo’s crew and therefore were in the possession of North Korea, the Navy had to assume that all keys being carried by the Pueblo had been compromised. Every ship and shore station in the Pacific theater (that is, several thousand installations, including ships at sea) had to replace all of their keys by physically carrying code books and punched cards to each installation.

The Pueblo incident was an extreme case. However, it has something in common with the problem of providing secure communication for commerce over the Internet. In both cases, codes are used for sending secure messages—not between two locations, but between a server (the Internet server or the Navy’s communications center) and a large number of communicants (individual web users or ships and shore stations). The more end users who are involved in the secure communications, the greater the problems of distribution and protection of the secret symmetric keys.

Although secure techniques for exchanging or creating symmetric keys can overcome this problem to some extent (for example, Diffie-Hellman key exchange, described later in this chapter), a more practical solution for use in computer communications came about with the invention of practical algorithms for asymmetric key cryptography.

Asymmetric Keys

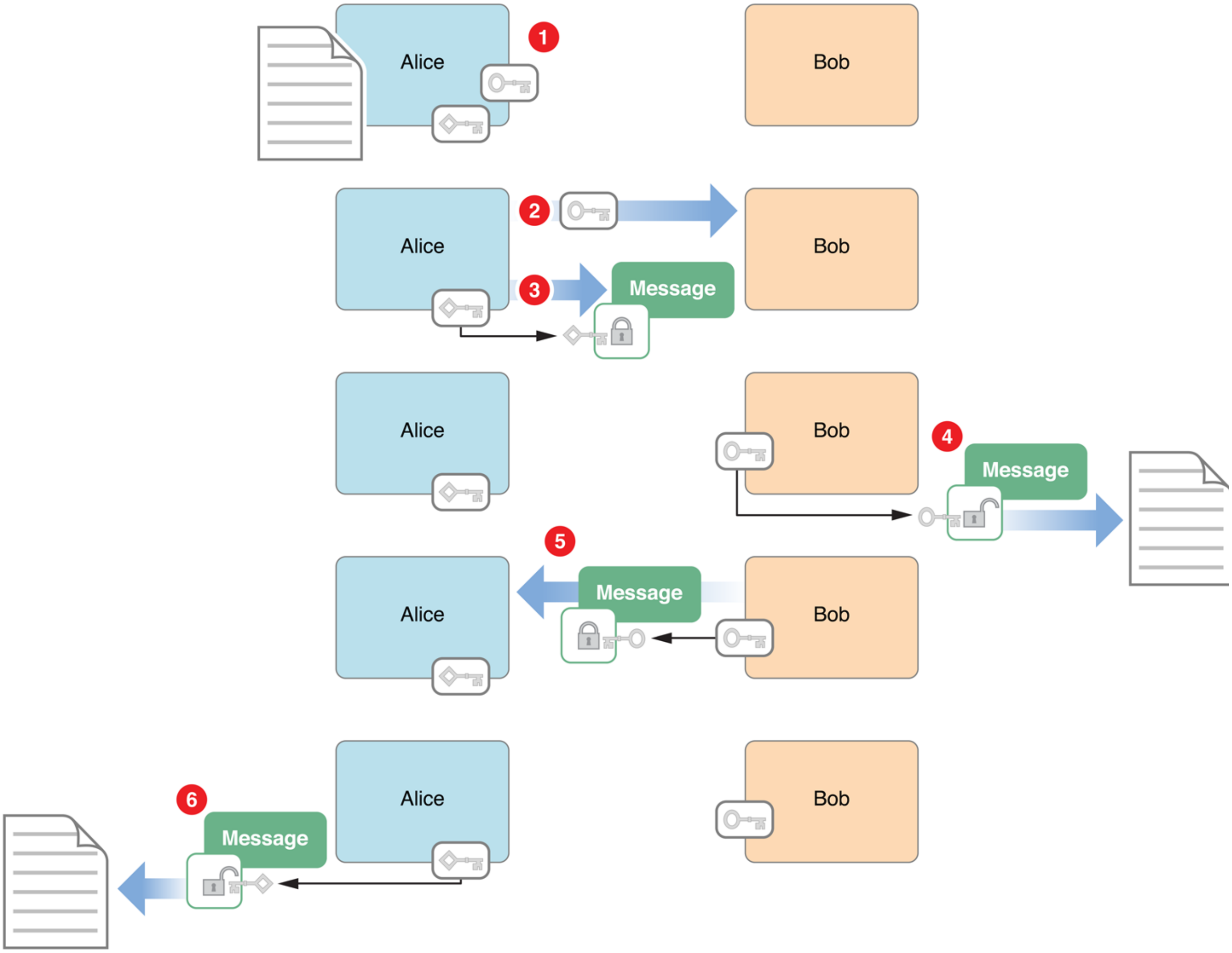
In asymmetric key cryptography, different keys are used for encrypting and decrypting a message. The asymmetric key algorithms that are most useful are those in which neither key can be deduced from the other. In that case, one key can be made public while the other is kept secure. This arrangement is often referred to as *public key cryptography*, and provides some distinct advantages over symmetric encryption: the necessity of distributing secret keys to large numbers of users is eliminated, and the algorithm can be used for authentication as well as for cryptography.

The first public key algorithm to become widely available was described by Ron Rivest, Adi Shamir, and Len Adleman in 1977, and is known as *RSA encryption* from their initials. Although other public key algorithms have been created since, RSA is still the most commonly used. The mathematics of the method are beyond the scope of this document, and are available on the Internet and in many books on cryptography. The algorithm is based on mathematical manipulation of two large prime numbers and their product. Its strength is believed to be related to the difficulty of factoring a very large number. With the current and foreseeable speed of modern digital computers, the selection of long-enough prime numbers in the generation of the RSA keys should make this algorithm secure indefinitely. However, this belief has not been proved mathematically, and either a fast factorization algorithm or an entirely different way of breaking RSA encryption might be possible. Also, if practical quantum computers are developed, factoring large numbers will no longer be an intractable problem.

Other public key algorithms, based on different mathematics of equivalent complexity to RSA, include ElGamal encryption and elliptic curve encryption. Their use is similar to RSA encryption (though the mathematics behind them differs), and they will not be discussed further in this document.

To see how public key algorithms address the problem of key distribution, assume that Alice wants to receive a secure communication from Bob. The procedure is illustrated in Figure 1-1.

Figure 1-1 Asymmetric key encryption



The secure message exchange illustrated in Figure 1-1 has the following steps:

1. Alice uses one of the public key algorithms to generate a pair of encryption keys: a private key, which she keeps secret, and a public key. She also prepares a message to send to Bob.
2. Alice sends the public key to Bob, unencrypted. Because her private key cannot be deduced from the public key, doing so does not compromise her private key in any way.
3. Alice can now easily prove her identity to Bob (a process known as *authentication*). To do so, she encrypts her message (or any portion of the message) using her private key and sends it to Bob.
4. Bob decrypts the message with Alice's public key. This proves the message must have come from Alice, as only she has the private key used to encrypt it.
5. Bob encrypts his message using Alice's public key and sends it to Alice. The message is secure, because even if it is intercepted, no one but Alice has the private key needed to decrypt it.
6. Alice decrypts the message with her private key.

Since encryption and authentication are subjects of great interest in national security and protecting corporate secrets, some extremely smart people are engaged both in creating secure systems and in trying to break them. Therefore, it should come as no surprise that actual secure communication and authentication procedures are considerably more complex than the one just described. For example, the authentication method of encrypting the message with your private key can be got around by a *man-in-the-middle attack*, in which someone with malicious intent (usually referred to as Eve in books on cryptography) intercepts Alice's original message and replaces it with their own, so that Bob is using not Alice's public key, but Eve's. Eve then intercepts each of Alice's messages, decrypts it with Alice's public key, alters it (if she wishes), and reencrypts it with her own private key. When Bob receives the message, he decrypts it with Eve's public key, thinking that the key came from Alice.

Although this is a subject much too broad and technical to be covered in detail in this document, digital certificates and digital signatures can help address these security problems. These techniques are described later in this chapter.

Diffie-Hellman Key Exchange

The *Diffie-Hellman key exchange* protocol is a way for two ends of a communication session to generate a shared symmetric key securely over an insecure channel. Diffie-Hellman is usually implemented using mathematics similar to RSA public key encryption. However, a similar technique can also be used with elliptic curve encryption. The basic steps are listed below:

1. Alice and Bob exchange public keys.
   - For RSA, these keys must have the same modulo portion, *p*.
   - For elliptic curve encryption, the domain parameters used for encryption must be agreed upon.

   As a rule, you should use the modulo or domain parameter values specified in RFC 5114.
2. Alice and Bob each encrypt a shared, non-secret value, *g*, using their private keys, and they exchange these encrypted values.

   The value for *g* is also usually taken from RFC 5114, but if another value is chosen when using RSA, the value for *g* must be a primitive root mod *p*—that is, any number that shares no common divisors with *p* other than 1, is congruent to a power of *g* mod *p*.
3. Alice encrypts the encrypted value received from Bob with her private key, and vice versa. These values are used as a shared session key.

At this point, even though neither side knows the other side's private key, both sides' session keys are identical. A third party intercepting the public keys but lacking knowledge of either private key cannot generate a session key. Therefore, data encrypted with the resulting session key is secure while in transit.

Although Diffie-Hellman key exchange provides strong protection against compromise of intercepted data, it provides no mechanism for ensuring that the entity on the other end of the connection is who you think it is. That is, this protocol is vulnerable to a man-in-the-middle attack. Therefore, it is sometimes used together with some other authentication method to ensure the integrity of the data.

Diffie-Hellman key exchange is supported by Apple Filing Protocol (AFP) version 3.1 and later and by Apple's Secure Transport API. Because RSA encryption tends to be slower than symmetric key methods, Diffie-Hellman (and other systems where public keys are used to generate symmetric private keys) can be useful when a lot of encrypted data must be exchanged.

Cryptographic Hash Functions

A *cryptographic hash function* takes any amount of data and applies an algorithm that transforms it into a fixed-size output value. For a cryptographic hash function to be useful, it has to be extremely difficult or impossible to reconstruct the original data from the hash value, and it must be extremely unlikely that the same output value could result from any other input data.

Sometimes it is more important to verify the integrity of data than to keep it secret. For example, if Alice sent a message to Bob instructing him to shred some records (legally, of course), it would be important to Bob to verify that the list of documents was accurate before proceeding with the shredding. Since the shredding is legal, however, there is no need to encrypt the message, a computationally expensive and time-consuming process. Instead, Alice could compute a hash of the message (called a *message digest*) and encrypt the digest with her private key. When Bob receives the message, he decrypts the message digest with Alice's public key (thus verifying that the message is from Alice) and computes his own message digest from the message text. If the two digests match, Bob knows the message has not been corrupted or tampered with.

The most common hash function you will use is SHA-1, an algorithm developed and published by the U.S. Government that produces a 160-bit hash value from any data up to 2**64 bits in length. There are also a number of more exotic algorithms such as SHA-2, elliptic-curve-based algorithms, and so on.

For compatibility with existing systems and infrastructure, you may occasionally need to use older algorithms such as MD5, but they are not recommended for use in new designs because of known weaknesses.

Digital Signatures

Digital signatures are a way to ensure the integrity of a message or other data using public key cryptography. Like traditional signatures written with ink on paper, they can be used to authenticate the identity of the signer of the data. However, digital signatures go beyond traditional signatures in that they can also ensure that the data itself has not been altered. This is like signing a check in such a way that if someone changes the amount of the sum written on the check, an "Invalid" stamp becomes visible on the face of the check.

Before a signer can create a digital signature, the signer must first have a digital *identity*—a public-private key pair and a corresponding digital certificate that proves the authenticity of the signer's public key.

The signer generates a message digest of the data and then uses the private key to encrypt the digest. The signer includes the encrypted digest and information about the signer's digital certificate along with the message. The combination of the encrypted digest and the digital certificate is a digital signature.

The certificate can later be used by the recipient to verify the signature; the certificate includes the public key needed to decrypt the digest and the algorithm used to create the digest. To verify that the signed document has not been altered, the recipient uses the same algorithm to create a digest of the message as received, then uses the public key to decrypt the encrypted digest from the message signature. If the two digests are identical, then the message cannot have been altered and must have been sent by the owner of the public key.

To ensure that the person who provided the signature is not only the same person who provided the data but is also who he or she claims to be, the certificate is also signed—in this case by the certification authority who issued the certificate. (More on certification authorities later.)

Digital signatures play a key role in code signing. Developers are encouraged to sign their apps. On execution, each app's signature is checked for validity. Digital signatures are required on all apps for iOS. Read *Code Signing Guide* for details about how code signing is used by OS X and iOS.

Figure 1-2 illustrates the creation of a digital signature.

Figure 1-2 Creating a digital signature

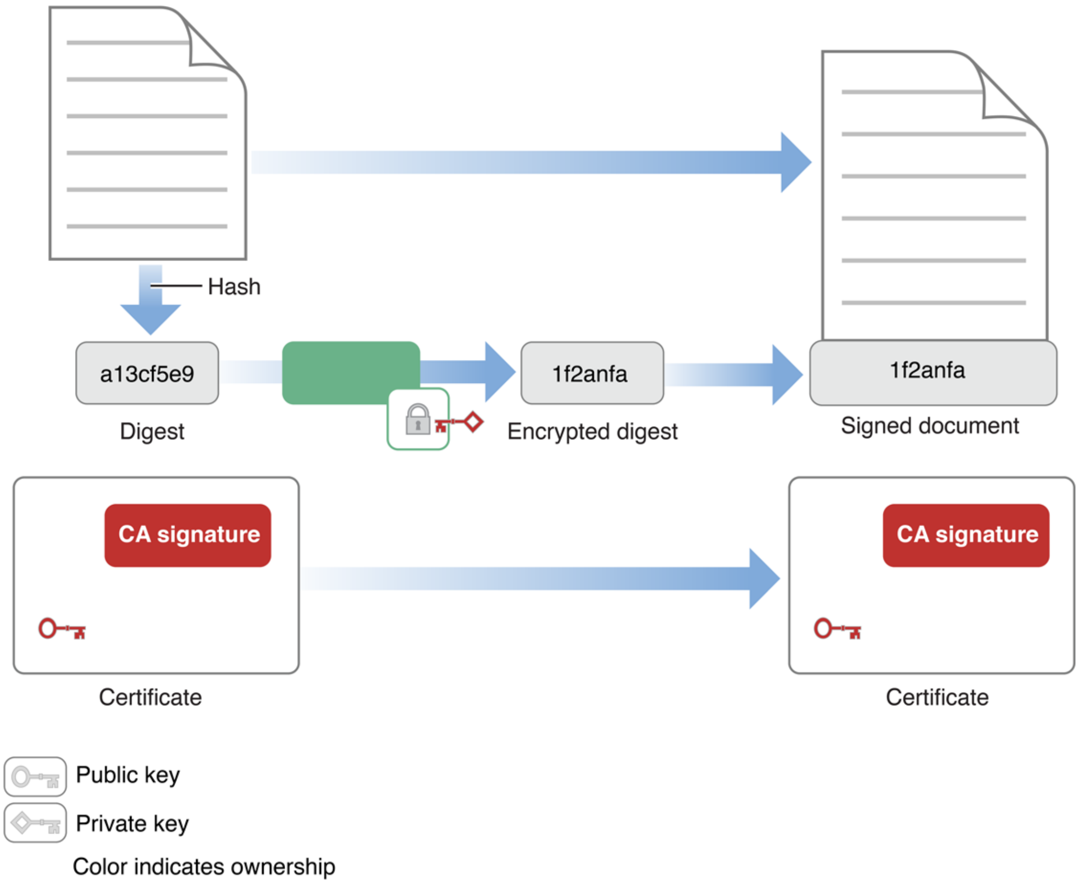
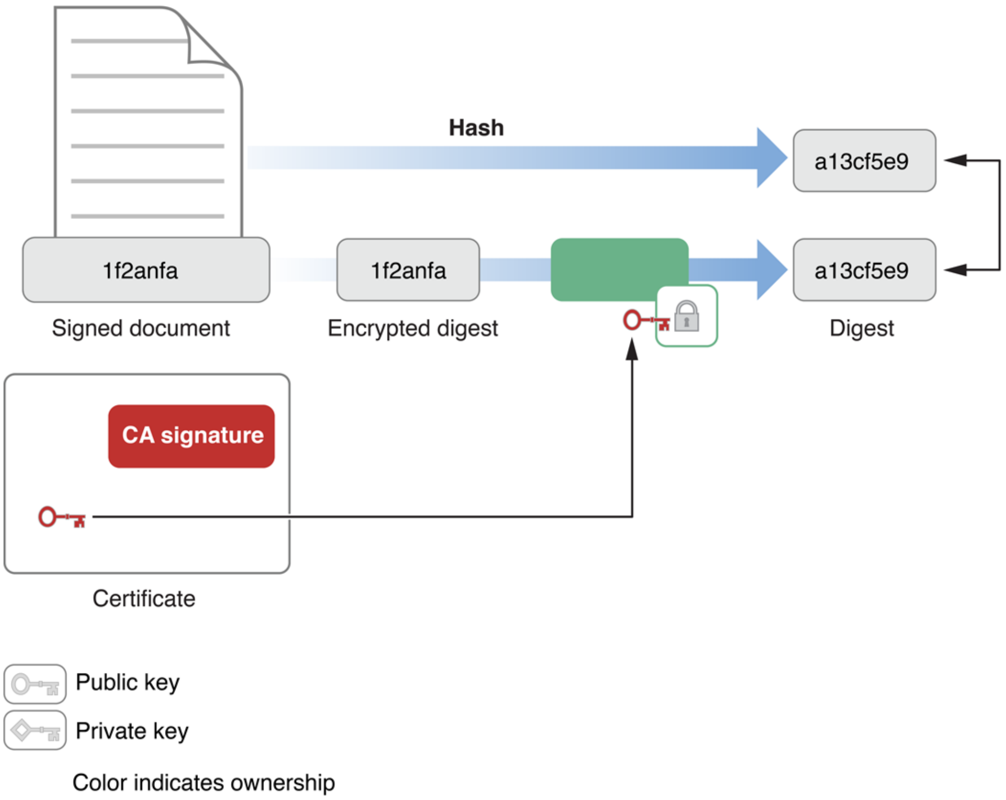


Figure 1-3 illustrates the verification of a digital signature. The recipient gets the signer's public key from the signer's certificate and uses that to decrypt the digest. Then, using the algorithm indicated in the certificate, the recipient creates a new digest of the data and compares the new digest to the decrypted copy of the one delivered in the signature. If they match, then the received data must be identical to the original data created by the signer.

Figure 1-3 Verifying a digital signature



Digital Certificates

A *digital certificate* is a collection of data used to verify the identity of the holder or sender of the certificate.

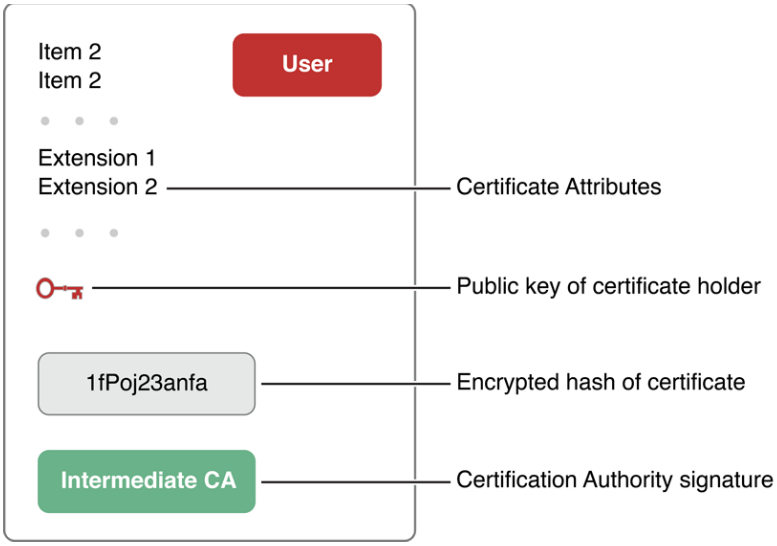
For example, an X.509 certificate contains such information as:

- Structural information—version, serial number, the message digest algorithm used to create the signature, and so on
- A digital signature from a *certification authority* (CA)—a person or organization that issued the certificate—to ensure that the certificate has not been altered and to indicate the identity of the issuer
- Information about the certificate holder—name, email address, company name, the owner's public key, and so on
- Validity period (the certificate is not valid before or after this period)
- *Certificate extensions*—attributes that contain additional information such as allowable uses for this certificate

The careful reader will have noticed that a digital signature includes the certificate of the signer, and that the signer's certificate, in turn, contains a digital signature that includes another certificate.

In general, each certificate is verified through the use of another certificate, creating a *chain of trust*—a chain of certificates, each of which is digitally signed by the next certificate in the chain, ending with a *root certificate*. The owner of this root certificate is called the *root certification authority*. Figure 1-4 illustrates the parts of a digital certificate.

Figure 1-4 Anatomy of a digital certificate


Item 2
Item 2
User
Extension 1
Extension 2
Certificate Attributes
Public key of certificate holder
1fPoj23anfa
Encrypted hash of certificate
Intermediate CA
Certification Authority signature

The root certificate is self-signed, meaning the signature of the root certificate was created by the root certification authority themselves. Figure 1-5 and Figure 1-6 illustrate how a chain of certificates is created and used. Figure 1-5 shows how the root certification authority creates its own certificate and then creates a certificate for a secondary certification authority.

Figure 1-5 Creating the certificates for the root CA and a secondary CA

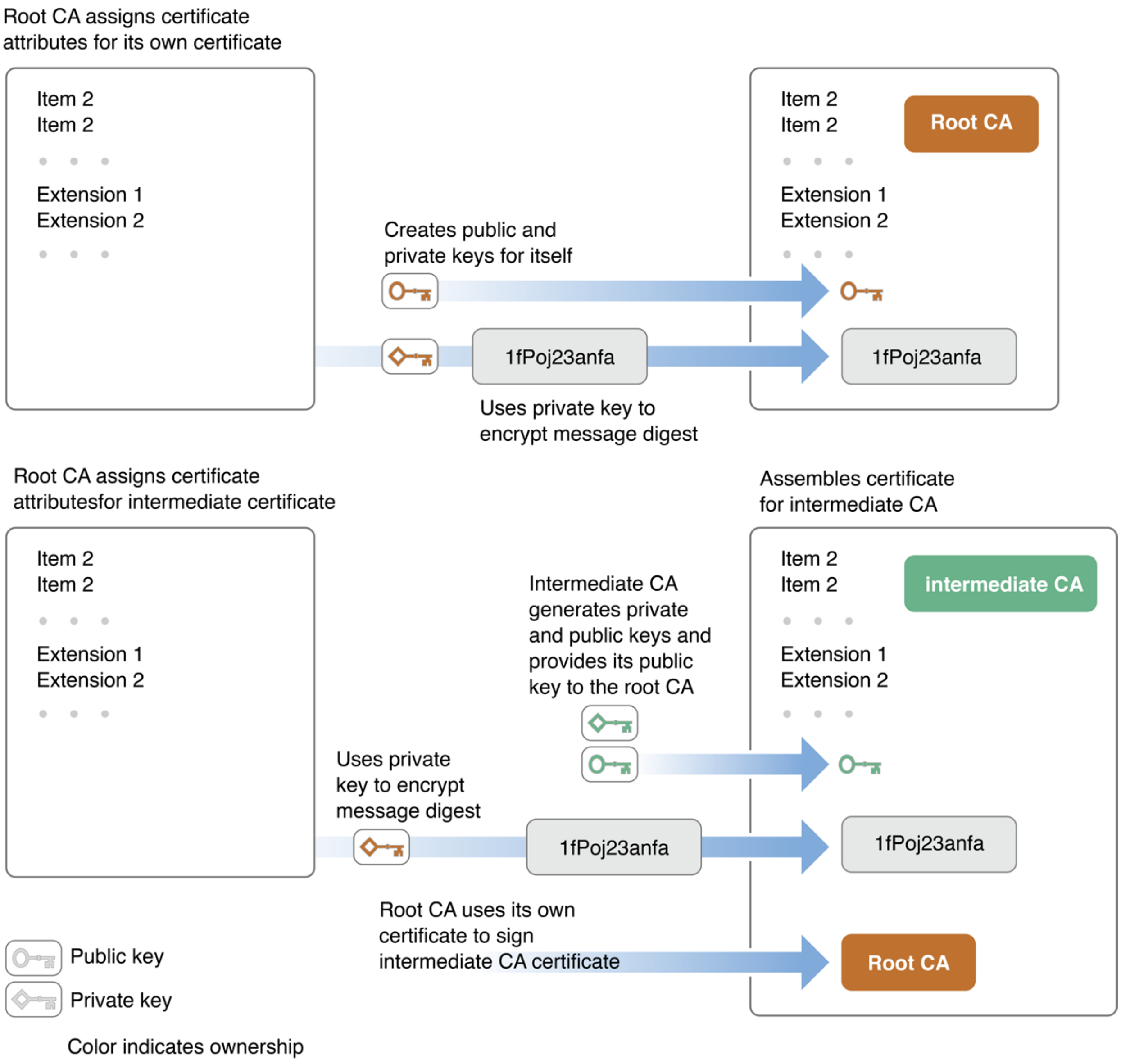
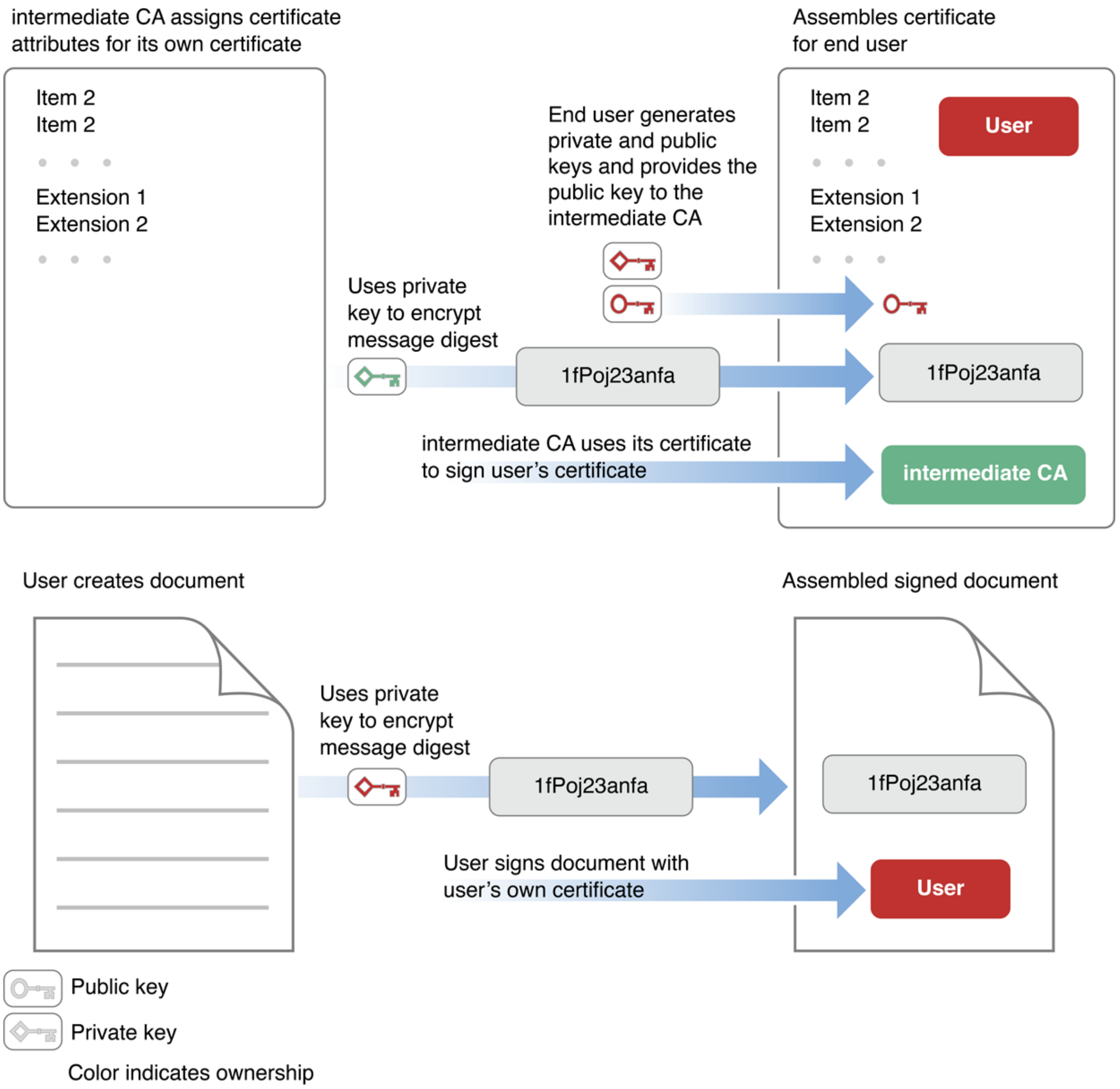

Root CA assigns certificate attributes for its own certificate
Item 2
Item 2
Extension 1
Extension 2
Creates public and private keys for itself
Root CA
Item 2
Item 2
Extension 1
Extension 2
1fPoj23anfa
1fPoj23anfa
Uses private key to encrypt message digest
Root CA assigns certificate attributesfor intermediate certificate
Assembles certificate for intermediate CA
Item 2
Item 2
Extension 1
Extension 2
Intermediate CA generates private and public keys and provides its public key to the root CA
intermediate CA
Item 2
Item 2
Extension 1
Extension 2
Uses private key to encrypt message digest
1fPoj23anfa
1fPoj23anfa
Root CA uses its own certificate to sign intermediate CA certificate
Root CA
Public key
Private key
Color indicates ownership

Figure 1-6 shows how the secondary certification authority creates a certificate for an end user and how the end user uses it to sign a document.

Figure 1-6 Creating the certificate for an end user and signing a document with it


intermediate CA assigns certificate attributes for its own certificate
Item 2
Item 2
Extension 1
Extension 2
End user generates private and public keys and provides the public key to the intermediate CA
Assembles certificate for end user
Item 2
Item 2
User
Extension 1
Extension 2
Uses private key to encrypt message digest
1fPoj23anfa
1fPoj23anfa
intermediate CA uses its certificate to sign user's certificate
intermediate CA
User creates document
Assembled signed document
Uses private key to encrypt message digest
1fPoj23anfa
1fPoj23anfa
User signs document with user's own certificate
User
Public key
Private key
Color indicates ownership

In Figure 1-6, the creator of the document has signed the document. The signature indicates the certificate of the document's creator (labeled User in the figure). The document's creator signs the document with a private key, and the signing certificate contains the corresponding public key, which can be used to decrypt the message digest to verify the signature (described earlier in Digital Signatures). This certificate—together with the private and public keys—was provided by a certification authority (CA).

In order to verify the validity of the user's certificate, the certificate is signed using the certificate of the CA. The certificate of the CA includes the public key needed to decrypt the message digest of the user's certificate. Continuing the certificate chain, the certificate of the CA is signed using the certificate of the authority who issued that certificate. The chain can go on through any number of intermediate certificates, but in Figure 1-5 the issuer of the CA's certificate is the root certification authority. Note that the certificate of the root CA, unlike the others, is self-signed—that is, it does not refer to a further certification authority but is signed using the root CA's own private key.

When a CA creates a certificate, it uses its private key to encrypt the certificate's message digest. The signature of every certificate the CA issues refers to its own signing certificate. The CA's public key is in this certificate, and the app verifying the signature must extract this key to verify the certificate of the CA. So it continues, on down the certificate chain, to the certificate of the root CA. When a root CA issues a certificate, it, too, signs the certificate. However, this signing certificate was not issued by another CA; the chain stops here. Rather, the root

CA issues its own signing certificate, as shown in Figure 1-5.

The certificate of the root CA can be verified by creating a digest and comparing it with one widely available. Typically, the root certificate and root CA's public key are already stored in the app or on the computer that needs to verify the signature.

It's possible to end a certificate chain with a trusted certificate that is not a root certificate. For example, a certificate can be certified as trusted by the user, or can be cross certified—that is, signed with more than one certificate chain. The general term for a certificate trusted to certify other certificates—including root certificates and others—is *anchor certificate*. Because most anchor certificates are root certificates, the two terms are often used interchangeably.

The confidence you can have in a given certificate depends on the confidence you have in the anchor certificate; for example, the trust you have in the certificate authorities and in their procedures for ensuring that subsequent certificate recipients in the certificate chain are fully authenticated. For this reason, it is always a good idea to examine the certificate that comes with a digital signature, even when the signature appears to be valid. In OS X and iOS, all certificates you receive are stored in your keychain. In OS X, you can use the Keychain Access utility to view them.

Certain attributes of a digital certificate (known as *certificate extensions*) provide additional information about the certificate. Some of these extensions describe how the certificate was intended to be used. For example, a certificate extension might indicate that a key can be used for code signing, or might provide a list of additional domain names for which a TLS certificate is valid. Other extensions provide signed time stamps indicating when the certificate was used to sign a particular document, thus allowing you to verify that a now-expired certificate was valid when it was used to sign the document. Still others provide information used for checking whether a certificate has been revoked. And so on.

These certificate extensions are interpreted in the context of a *trust policy*—a set of rules that specify how a particular extension affects whether the certificate should be trusted for a given use. For example, a trust policy might specify that in order to be trusted to verify a digitally signed email message, a certificate must contain an email address that matches the address of the sender of the email.

Exhibit 26

Encrypting and Hashing Data

Both symmetric and asymmetric key encryption schemes can be used to encrypt data. Asymmetric encryption is most commonly used for sending data across trust boundaries, such as one person sending another person an encrypted email. It is also often used for sending a symmetric session key across an insecure communication channel so that symmetric encryption can then be used for future communication. Symmetric encryption is most commonly used for data at rest (on your hard drive for example) and as a session key in a number of encrypted networking schemes.

OS X and iOS provide a number of different APIs for encryption and decryption. This chapter describes the recommended APIs.

Encryption Technologies Common to iOS and OS X

OS X and iOS provide a number of encryption technologies. Of these, three APIs are available on both iOS and OS X:

- Keychain Services API—provides secure storage for passwords, keys, and so on
- Cryptographic Message Syntax—provides (nonstreaming) symmetric and asymmetric encryption and decryption
- Certificate, Key, and Trust Services—provides cryptographic support services and trust validation

The sections that follow describe these technologies.

Keychain Services

The Keychain Services API is commonly used to store passwords, keys, certificates, and other secrets in a special encrypted file called a keychain. You should always use the keychain to store passwords and other short pieces of data (such as cookies) that are used to grant access to secure web sites, as otherwise this data might be compromised if an unauthorized person gains access to a user's computer, mobile device, or a backup thereof.

Although this is mostly used for storing passwords and keys, the keychain can also store small amounts of arbitrary data. The keychain is described further in Managing Keys, Certificates, and Passwords.

OS X also includes a utility that allows users to store and read the data in the keychain, called *Keychain Access*. For more information, see Keychain Access in *Security Overview*.

Cryptographic Message Syntax Services

The Cryptographic Message Syntax Services programming interface allows you to encrypt or add a digital signature to S/MIME messages. (S/MIME is a standard for encrypting and signing messages, most commonly used with email.) It is a good API to use when signing or encrypting data for store–

and-forward applications, such as email. See *Cryptographic Message Syntax Services Reference* for details.

Certificate, Key, and Trust Services

The Certificate, Key, and Trust Services API provides trust validation and support functions for cryptography. These features are described further in Managing Keys, Certificates, and Passwords.

In iOS, this API also provides basic encryption capabilities, as described in Encryption in iOS.

Common Crypto

In OS X v10.5 and later and iOS 5.0 and later, Common Crypto provides low-level C support for encryption and decryption. Common Crypto is not as straightforward as Security Transforms, but provides a wider range of features, including additional hashing schemes, cipher modes, and so on.

For more information, see the manual page for `CommonCrypto`.

Encryption Technologies Specific to OS X

In addition to Keychain Services and Cryptographic Message Syntax Services, OS X provides four additional APIs for performing encryption:

- Security Transforms API—a Core-Foundation-level API that provides support for signing and verifying, symmetric cryptography, and Base64 encoding and decoding
- Common Crypto—a C-level API that can perform most symmetric encryption and decryption tasks
- CDSA/CSSM—a legacy API that should be used only to perform tasks not supported by the other two APIs, such as asymmetric encryption

These APIs are described in the sections that follow.

Security Transforms

In OS X v10.7 and later, the Security Transforms API provides efficient and easy-to-use support for performing cryptographic tasks. Security transforms are the recommended way to perform symmetric encryption and decryption, asymmetric signing and verifying, and Base64 encoding and decoding in OS X.

Based on the concept of data flow programming, the Security Transforms API lets you construct graphs of transformations that feed into one another, transparently using Grand Central Dispatch to schedule the resulting work efficiently across multiple CPUs. As the `CFDataRef` (or `NSData`) objects pass through the object graph, callbacks within each individual transform operate on that data, then pass it on to the transform's output, which may be connected to the input of another transform object, and so on.

The transform API also provides a file reader transform (based on `CFReadStreamRef` or `NSInputStream` objects) that can be chained to the input of other transforms.

Using the built-in transforms, the Security Transforms API allows you to read files, perform symmetric encryption and decryption, perform asymmetric signing and verifying, and perform Base64 encoding. The Security Transforms API also provides support for creating custom transforms that perform other operations on data. For example, you might create a transform that byte swaps data prior to encrypting it or a transform that encodes the resulting encrypted data for transport.

For more information, read *Security Transforms Programming Guide* and *Security Transforms Reference*.

CDSA/CSSM

> **Important:** CDSA (including CSSM) is deprecated and should not be used for new development. It is not available in iOS.

CDSA is an Open Source security architecture adopted as a technical standard by the Open Group. Apple has developed its own Open Source implementation of CDSA, available as part of Darwin at Apple's Open Source site. This API provides a wide array of security services, including fine-grained access permissions, authentication of users' identities, encryption, and secure data storage.

Although CDSA has its own standard programming interface, it is complex and does not follow standard Apple programming conventions. For this reason, the CDSA API is deprecated as of OS X version 10.7 (Lion) and is not available in iOS. Fortunately, OS X and iOS include their own higher-level security APIs that abstract away much of that complexity.

Where possible, you should use one of the following instead of using CDSA directly:

- The Security Objective-C API for authentication (in OS X). See Security Objective-C API in *Security Overview* for details.
- The Security Transforms API for symmetric encryption and decryption, asymmetric signing and verifying, and other supported tasks in OS X v10.7 and later. See Security Transforms for details.
- The Certificate, Key, and Trust Services API for general encryption, key management, and other tasks. See Encryption in iOS for details.

If these APIs do not meet your needs, you can still use CDSA in OS X, but please file bugs at http://bugreport.apple.com/ to request the additional functionality that you need. For more information, read CDSA Overview.

OpenSSL

Although OpenSSL is commonly used in the open source community, OpenSSL does not provide a stable API from version to version. For this reason, although OS X provides OpenSSL libraries, the OpenSSL libraries in OS X are deprecated, and OpenSSL has never been provided as part of iOS. Use of the OS X OpenSSL libraries by apps is strongly discouraged.

If your app depends on OpenSSL, you should compile OpenSSL yourself and statically link a known version of OpenSSL into your app. This use of OpenSSL is possible on both OS X and iOS. However, unless you are trying to maintain source compatibility with an existing open source project, you should generally use a different API.

Common Crypto and Security Transforms are the recommended alternatives for general encryption. CFNetwork and Secure Transport are the recommended alternatives for secure communications.

Encryption in iOS

In iOS, in addition to providing support functions for encoding and decoding keys, the Certificate, Key, and Trust Services API also provides basic encryption, decryption, signing, and verifying of blocks of data using the following `SecKey` functions:

`SecKeyEncrypt`—encrypts a block of data using the specified key.

`SecKeyDecrypt`—decrypts a block of data using the specified key.

`SecKeyRawSign`—signs a block of data using the specified key.

`SecKeyRawVerify`—verifies a signature against a block of data and a specified key.

You can find examples of how to use these functions in Certificate, Key, and Trust Services Tasks for iOS in *Certificate, Key, and Trust Services Programming Guide*.

For detailed reference content, read *Certificate, Key, and Trust Services Reference*.

Exhibit 27

Managing Keys, Certificates, and Passwords

The *keychain* provides storage for passwords, encryption keys, certificates, and other small pieces of data. After an app requests access to a keychain, it can store and retrieve sensitive data, confident that untrusted apps cannot access that data without explicit action by the user.

In OS X, the user is prompted for permission when an app needs to access the keychain; if the keychain is locked, the user is asked for a password to unlock it.

In iOS, an app can access only its own items in the keychain—the user is never asked for permission or for a password.

There are two recommended APIs for accessing the keychain:

- Certificate, Key, and Trust Services
- Keychain Services

Certificate, Key, and Trust Services

Certificate, Key, and Trust Services is a C API for managing certificates, public and private keys, symmetric keys, and trust policies in iOS and OS X. You can use these services in your app to:

- Create certificates and asymmetric keys
- Add certificates and keys to keychains, remove them from keychains, and use keys to encrypt and decrypt data
- Retrieve information about a certificate, such as the private key associated with it, the owner, and so on
- Convert certificates to and from portable representations
- Create and manipulate trust policies and evaluate a specific certificate using a specified set of trust policies
- Add anchor certificates

In OS X, functions are also available to retrieve anchor certificates and set user-specified settings for trust policies for a given certificate.

In iOS, additional functions are provided to:

- Use a private key to generate a digital signature for a block of data
- Use a public key to verify a signature
- Use a public key to encrypt a block of data
- Use a private key to decrypt a block of data

Certificate, Key, and Trust Services operates on certificates that conform to the X.509 ITU standard, uses the keychain for storage and retrieval of certificates and keys, and uses the trust policies provided by Apple.

Because certificates are used by SSL and TLS for authentication, the Secure Transport API includes a variety of functions to manage the use of certificates and root certificates in a secure connection.

To display the contents of a certificate in an OS X user interface, you can use the `SFCertificatePanel` and `SFCertificateView` classes in the Security Objective-C API. In addition, the `SFCertificateTrustPanel` class displays trust decisions and lets the user edit trust decisions.

Keychain Services

In OS X and iOS, Keychain Services allows you to create keychains, add, delete, and edit keychain items, and—in OS X only—manage collections of keychains. In most cases, a keychain-aware app does not have to do any keychain management and only has to call a few functions to store or retrieve passwords.

By default, backups of iOS data are stored in cleartext, with the exception of passwords and other secrets on the keychain, which remain encrypted in the backup. It is therefore important to use the keychain to store passwords and other data (such as cookies) that are used to access secure web sites. Otherwise, this data might be compromised if an unauthorized person gains access to the backup data.

To get started using Keychain Services, see *Keychain Services Programming Guide* and *Keychain Services Reference*.

In OS X, the Keychain Access application provides a user interface to the keychain. See Keychain Access in *Security Overview* for more information about this application.

To Learn More

For more information about using Keychain Services to store and retrieve secrets and certificates, read *Keychain Services Programming Guide* and *Keychain Services Reference*.

For more information about Secure Transport, read Secure Transport.

For more information about the certificate user interface API, read Security Objective-C API in *Security Overview*.

Exhibit 28

Glossary

anchor certificate A digital certificate trusted to be valid, which can then be used to verify other certificates. An anchor certificate can be a root certificate, a cross-certified certificate (that is, a certificate signed with more than one certificate chain), or a locally defined source of trust.

CDSA Abbreviation for Common Data Security Architecture. An open software standard for a security infrastructure that provides a wide array of security services, including fine-grained access permissions, authentication of users, encryption, and secure data storage. CDSA has a standard application programming interface, called CSSM. In addition, OS X includes its own security APIs that call the CDSA API for you.

certificate See digital certificate.

certificate chain See chain of trust.

certificate extension A data field in a digital certificate containing information such as allowable uses for the certificate.

Certificate, Key, and Trust Services An API you can use to create, manage, and read certificates; add certificates to a keychain; create encryption keys; and manage trust policies. In iOS, you can also use this API to encrypt, decrypt, and sign data.

certification authority (CA) The issuer of a digital certificate. In order for the digital certificate to be trusted, the certification authority must be a trusted organization that authenticates an applicant before issuing a certificate.

chain of trust A set of digital certificates in which each certificate signs the next certificate, ending in a root certificate that is also a trusted anchor certificate. A chain of trust can be used to verify the validity of a digital certificate.

cipher A scheme for encrypting data.

ciphertext Text or other data that has been encrypted. Compare cleartext.

cleartext Ordinary, unencrypted data. Compare ciphertext.

cryptographic hashing The process whereby data is transformed into a much smaller value that can take the place of the original data for cryptographic purposes. A hashing algorithm takes any amount of data and transforms it into a fixed-size output value. For a cryptographic hash function to be useful for security, it has to be extremely difficult or impossible to reconstruct the original data from the hash value, and it must be extremely unlikely that the same output value could result from any similar input data. See also message digest.

CSSM Abbreviation for Common Security Services Manager. A public application programming interface for CDSA. CSSM also defines an interface for plug-ins that implement security services for a particular operating system and hardware environment.

decryption The transformation of encrypted data back into the original cleartext. Compare encryption.

Diffie-Hellman key exchange A protocol that provides a way for two ends of a communication session to generate a symmetric shared secret key through the exchange of public keys.

digest See message digest.

digital certificate A collection of data used to verify the identity of the holder or sender of the certificate. OS X and iOS support the X.509 standard for digital certificates. See also certificate chain.

digital signature A way to ensure the integrity of a message or other data using public key cryptography. To create a digital signature, the signer generates a message digest of the data and then uses a private key to encrypt the digest. The signature includes the encrypted digest and identifies the signer. Anyone wanting to verify the signature uses the signer's digital certificate, which contains the public key needed to decrypt the digest and specifies the algorithm used to create the digest.

encryption The transformation of data into a form in which it cannot be made sense of without the use of some key. Such transformed data is referred to as *ciphertext*. Use of a key to reverse this process and return the data to its original (cleartext) form is called decryption.

hash algorithm See cryptographic hashing.

identity A digital certificate together with an associated private key.

keychain A database in OS X and iOS used to store encrypted passwords, private keys, and other secrets. It is also used to store certificates and other non-secret information that is used in cryptography and authentication. Apps can use the Keychain Services API (or the legacy Keychain Manager API) to manipulate data in the keychain. Users can also access keychain data using the Keychain Access utility.

man-in-the-middle attack An attack on a communication channel in which the attacker can intercept messages going between two parties without the communicating parties' knowledge. Typically, the man in the middle substitutes messages and even cryptographic keys to impersonate one party to the other.

message digest The result of applying a cryptographic hash function to a message or other data. A cryptographically secure message digest cannot be transformed back into the original message and cannot (or is very unlikely to) be created from a different input. Message digests are used to ensure that a message has not been corrupted or altered. For example, they are used for this purpose in digital signatures. The digital signature includes a digest of the original message, and the recipient prepares their own digest of the received message. If the two digests are identical, then the recipient can be confident that the message has not been altered or corrupted.

plaintext See cleartext.

private key A cryptographic key that must be kept secret, usually used in the context of public key cryptography. Although this term can also be used in the context of symmetric key cryptography, the term "secret key" (or "shared secret") is preferred.

pseudorandom number A number generated by an algorithm that produces a series of numbers with no discernible pattern. It should be impossible or nearly impossible to deduce the algorithm from such a series. However, unlike a truly random number generator, a pseudorandom number generator always produces the same series if the algorithm is given the same starting value or values.

public-private key pair A pair of mathematically related keys that cannot be derived from one another used in public key cryptography. One of these keys (the public key) is made public while the other (the private key) is kept secure. Data encrypted with one key must be decrypted with the other.

public key A cryptographic key that can be shared or made public without compromising the cryptographic method—generally, the public portion of a public-private key pair. See also public key cryptography.

public key certificate See digital certificate.

public key cryptography A cryptographic method using a public-private key pair. If the public key is used to encrypt the data, only the holder of the private key can decrypt it; therefore the data is secure from unauthorized use. If the private key is used to encrypt the data, anyone with the public key can decrypt it. Because only the holder of the private key could have encrypted it, such data can be used for authentication. See also digital certificate; digital signature. Compare symmetric key cryptography.

root certificate A certificate that can be verified without recourse to another certificate. Rather than being signed by a further certification authority (CA), a root certificate is verified using the widely available public key of the CA that issued the root certificate. Compare anchor certificate.

root certification authority The certification authority that owns the root certificate.

RSA encryption A system of public key cryptography, named for its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm takes two large prime numbers, finds their product, and then derives a public-private key pair from the prime numbers and their product. The strength of this algorithm depends on the difficulty of factoring the resulting product and upon reasonable assurance of the primality of the values used in constructing the keys.

secret key A cryptographic key that cannot be made public without compromising the security of the cryptographic method. In symmetric key cryptography, a secret key is used both to encrypt and decrypt data, and is often called a *shared secret*. Although the term “secret key” can be used in the context of public key cryptography, the term “private key” is preferred.

Secure Sockets Layer (SSL) A protocol that provides secure communication over a TCP/IP connection such as the Internet. It uses digital certificates for authentication and digital signatures to ensure message integrity, and can use public key cryptography to ensure data privacy. An SSL service negotiates a secure session between two communicating endpoints. SSL is built into all major browsers and web servers. SSL has been superseded by Transport Layer Security (TLS).

secure storage Storage of encrypted data on disk or another medium that persists when the power is turned off.

Secure Transport The OS X and iPhone implementation of Secure Sockets Layer (SSL) and

Transport Layer Security (TLS), used to create secure connections over TCP/IP connections such as the Internet. Secure Transport includes an API that is independent of the underlying transport protocol. The CFNetwork and URL Loading System APIs use the services of Secure Transport.

session key A cryptographic key calculated or issued for use only for the duration of a specific communication session. Session keys are used, for example, by the SSL and Kerberos protocols, and are often obtained using Diffie-Hellman key exchange.

SSL See Secure Sockets Layer (SSL).

strength A measure of the amount of effort required to break a security system. For example, the strength of RSA encryption is believed to be related to the difficulty of factoring the product of two large prime numbers.

symmetric key cryptography Cryptography that uses a single shared key to encrypt and decrypt data. See also secret key. Compare public key cryptography.

TLS See Transport Layer Security (TLS).

Transport Layer Security (TLS) A protocol that provides secure communication over a TCP/IP connection such as the Internet. It uses certificates for authentication and signatures to ensure message integrity, and can use public key cryptography to ensure data privacy. A TLS service negotiates a secure session between two communicating endpoints. TLS is built into recent versions of all major browsers and web servers. TLS is the successor to SSL. Although the TLS and SSL protocols are not interoperable, Secure Transport can back down to SSL 3.0 if a TLS session cannot be negotiated.

trust policy A set of rules that specify the appropriate uses for a certificate based on its certificate extensions and other trust criteria. For example, a standard trust policy specifies that the user should be prompted for permission to trust an expired certificate. However, a custom trust policy might override that behavior in some specific set of circumstances, such as when verifying the signature on a document that you know was generated while the certificate was still valid.

X.509 A standard for digital certificates promulgated by the International Telecommunication Union (ITU). The X.509 ITU standard is widely used on the Internet and throughout the information technology industry for designing secure apps based on a public key infrastructure (PKI).

Exhibit 29

Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues

This article is about adverse issues experienced by customers who have made unauthorized modifications to iOS (this hacking process is often called "jailbreaking").

iOS is designed to be reliable and secure from the moment you turn on your device. Built-in security features protect against malware and viruses and help to secure access to personal information and corporate data. Unauthorized modifications to iOS ("jailbreaking") bypass security features and can cause numerous issues to the hacked iPhone, iPad, or iPod touch, including:

Security vulnerabilities: Jailbreaking your device eliminates security layers designed to protect your personal information and your iOS device. With this security removed from your iOS device, hackers may steal your personal information, damage your device, attack your network, or introduce malware, spyware or viruses.

Instability: Frequent and unexpected crashes of the device, crashes and freezes of built-in apps and third-party apps, and loss of data.

Shortened battery life: The hacked software has caused an accelerated battery drain that shortens the operation of an iPhone, iPad, or iPod touch on a single battery charge.

Unreliable voice and data: Dropped calls, slow or unreliable data connections, and delayed or inaccurate location data.

Disruption of services: Services such as Visual Voicemail, Weather, and Stocks have been disrupted or no longer work on the device. Additionally, third-party apps that use the Apple Push Notification Service have had difficulty receiving notifications or received notifications that were intended for a different hacked device. Other push-based services such as iCloud and Exchange have experienced problems synchronizing data with their respective servers.

Inability to apply future software updates: Some unauthorized modifications have caused damage to iOS that is not repairable. This can result in the hacked iPhone, iPad, or iPod touch becoming permanently inoperable when a future Apple-supplied iOS update is installed.

Apple strongly cautions against installing any software that hacks iOS. It is also important to note that unauthorized modification of iOS is a violation of the iOS end-user software license agreement and because of this, Apple may deny service for an iPhone, iPad, or iPod touch that has installed any unauthorized software.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Risks are inherent in the use of the Internet. Contact the vendor for additional information. Other company and product names may be trademarks of their respective owners.

Last Modified: Sep 22, 2015

Helpful? Yes No

82% of people found this helpful.

Additional Product Support Information

iPod touch

iPod

iPad

Start a Discussion

in Apple Support Communities

Ask other users about this article

Submit my question to the community

See all questions on this article   See all questions I have asked

Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.
Get started

Support   Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues

More ways to shop: Visit an Apple Store, call 1-800-MY-APPLE, or find a reseller.

Privacy Policy | Terms of Use | Sales and Refunds | Site Map | Contact Apple   United States (English)

Exhibit 30

Code Signing

Code signing your app assures users that it is from a known source and the app hasn't been modified since it was last signed. Before your app can integrate app services, be installed on a device, or be submitted to the App Store, it must be signed with a certificate issued by Apple. For more information on how to request certificates and code sign your apps, review the App Distribution Guide.

Common Tasks

To avoid potential issues with common tasks involving code signing, follow these best practices:

Signing and Running Development Builds

- Launching Your iOS App on a Device
- Launching Your Mac App

Beta Testing

- Beta Testing Your iOS App
- How to reproduce bugs reported against Mac App Store submissions

Distribution

- Submitting Your App
- Distributing Enterprise Apps for iOS Devices (in-house, internal use)

Essential Guides and Documentation

- App Distribution Guide
- Code Signing Troubleshooting
- Troubleshooting Push Notifications
- Developer ID and Gatekeeper (OS X)
- Code Signing Guide (OS X)

Frequently Asked Questions

- **How do I transfer my code signing certificates and provisioning profiles to another Mac?**
  Review the instructions in
  Exporting and Importing Certificates and Provisioning Profiles.

- **What does “Valid Signing Identity Not Found” mean and how do I resolve it?**
  Follow the steps outlined in
  Your Certificates Are Invalid Because You're Missing Private Keys.

- **How do I resolve a code signing build error?**
  See the list of published solutions in Build and Code Signing Issues.

- **How do I revoke or delete my certificates and start over?**
  Use the process outlined in
  Re-Creating Certificates and Updating Related Provisioning Profiles.

- **Do I need to define a custom Code Signing Entitlements file in Xcode?**
  To understand when entitlements are required and how to configure them properly, see Adding Capabilities.

Apple Developer Forum Discussions

- Capabilityies, Certificates, Identifiers & Profiles
- App Submission and Review

Developer Forums

Post questions and share thoughts with fellow developers and Apple engineers.

Discuss with other developers

Contact Us

Get personalized help with enrollment, membership, tools, and more.

Contact Apple Developer Support