COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER and

CONSUMER WATCHDOG

To

THE FEDERAL COMMUNICATIONS COMMISSION

Privacy and Security of Information Stored on Mobile Communications Devices

"CC Docket No. 96–115; DA 12–818"

July 13, 2012

By notice published on June 13, 2012, the Federal Communications Commission ("FCC") seeks comments on "privacy and data security practices of mobile wireless services providers with respect to customer information stored on their users' mobile communications devices."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC"), and Consumer Watchdog submit these comments and recommendations to ensure that the proposed rule ensures that carriers adequately protect the privacy of consumers' personal information.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FCC. In 2001, EPIC recommended that the Commission initiate a rulemaking proceeding to establish fair location information practices.[2] In 2007, EPIC and other consumer groups urged the Commission to promulgate further safeguards for protecting customers' Customer Proprietary Network Information ("CPNI").[3] Most recently, EPIC called on the Commission to investigate

[1] Privacy and Security of Information Stored on Mobile Communications Devices, 77 Fed. Reg. 35336 (proposed June 13, 2012), http://www.gpo.gov/fdsys/pkg/FR-2012-06-13/pdf/2012-14496.pdf.
[2] CTIA Petition for Rulemaking to Establish Fair Location Information Practices, *Comments of the Electronic Privacy Information Center*, (Apr. 6, 2001), *available at* https://epic.org/privacy/wireless/epic_comments.pdf.
[3] Further Notice of Proposed Rulemaking: Customer Proprietary Network Information, *Comments of the Consumer Coalition*, (Jul. 9, 2007), *available at* https://epic.org/privacy/cpni/cpni_070607.pdf.

Google's interception of Wi-Fi payload data from private, residential networks—an investigation that ultimately produced a $25,000 fine.[4]

Consumer Watchdog is a tax-exempt 501(c)(3) nonprofit organization dedicated to educating and advocating on behalf of consumers for over 25 years. Through policy research, investigation, public education, advocacy (including litigation), and direct consumer outreach, Consumer Watchdog has helped millions of Americans save billions of dollars on their insurance bills, secure the quality health care they need, and, for low-income consumers, gain access to important programs. Consumer Watchdog's public education and advocacy efforts work to expose, confront, and change deceptive practices. Our advocates field complaints from consumers nationwide and work with regulators, policymakers and consumer protection agencies to improve laws and regulations to better protect consumers from deceptive corporate conduct, anti-competitive behavior, and corporate abuse.

The Commission requests comments on the following questions: "Are consumers given meaningful notice and choice with respect to service providers' collection of usage-related information on their devices? . . . Do current practices raise concerns with respect to consumer privacy and data security?" EPIC recommends that the Commission require mobile carriers to implement comprehensive privacy and security protections based on Fair Information Practices. The President has recently set out a technology-neutral framework for privacy protection—the Consumer Privacy Bill of Rights ("CPBR")—that would require companies that collect and use personal data on consumers to take on privacy responsibilities and provide enhanced privacy and

[4] Letter from Marc Rotenberg, Executive Director, Electronic Privacy Information Center, to Julius Genachowski, Chairman, Federal Communications Commission, May 18, 2010, https://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf.

security protections.[5] The CPBR provides a good core around which the Commission can develop Fair Information Practices for carriers.

Section I provides an overview of current mobile privacy issues. Section II outlines the Consumer Privacy Bill of Rights. Finally, Section III applies the CPBR principles to mobile service providers.

I. Privacy Risks Created by the Collection and Disclosure of Consumer Information

As the Commission notes, "the issue of customer information on mobile devices has recently gained greater prominence."[6] Currently, mobile carriers are capable of collecting a wide range of information about consumer use of cell phones and apps. For example, Verizon Wireless collects location data, web addresses and search terms, demographic information, amount of usage of the mobile phone, and type of data plan used by the consumer.[7] By virtue of their access to the Internet usage history of smartphone users, mobile carriers are capable of building extensive digital profiles of individual consumers.[8] These profiles may contain sensitive information about the consumer, including health or financial data and information revealing the individual's exercise of First Amendment rights.[9]

Although mobile carriers claim to collect and store data primarily to improve mobile service to the user,[10] carriers also use and share data for unrelated purposes. Mobile carriers collect, store, and then share data with third parties for use in behavioral advertising, in which

---

[5] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter White House, CPBR].
[6] Privacy and Security of Information Stored on Mobile Communications Devices, *supra* note 1, at 35337.
[7] *Privacy Policy*, VERIZON WIRELESS, http://www22.verizon.com/about/privacy/policy/ (last visited June 21, 2012 at 5:17PM) [hereafter "Verizon Privacy Policy"].
[8] *See, generally*, SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE DIGITAL AGE (2004); *see also*, White House, CPBR at 11; EPIC, *Privacy and Consumer Profiling*, http://epic.org/privacy/profiling/default.html (last visited, June 25, 2012).
[9] White House, CPBR at 11.
[10] *See, e.g.* Verizon Privacy Policy.

information about the consumer's online interests is used to allow companies to target advertisements to the consumer.[11] Advertisers might categorize an individual as a potential car buyer, sports enthusiast, or expectant mother based on the individual's smartphone Internet search.[12] Since the 1980s, marketers have used aggregated information about consumers—provided by first person providers of services or products, such as the mobile carriers at issue here—to compile consumer profiles.[13]

Use of consumer data to develop predictive models for targeted advertising threatens privacy. First, despite anonymization and aggregation, consumer profiles represent a form of surveillance.[14] Second, although all four mobile carriers pledge to share information only in aggregated or anonymous form, deidentified information may be easily re-identified with a specific person downstream.[15] Famously, data analysts re-identified anonymized Netflix movie recommendations within two weeks of the data set's release by cross-referencing the data set with publicly available resources online.[16] Given the ease with which anonymized information may be re-identified, consumer data collected by carriers might be only temporarily safeguarded. Additionally, because mobile carriers bear no legal responsibility for the downstream uses of consumer data, they have few incentives to ensure that third parties respect the context in which consumers agreed to the collection of their data.

[11] White House, CPBR at 12.
[12] Miguel Helft, Google to Offer Ads Based on Interests, N.Y. TIMES, Mar. 11, 2009, *available at* http://www.nytimes.com/2009/03/11/technology/internet/11google.html?_r=1.
[13] Solove, *supra* note 8, at 19.
[14] Solove, *supra* note 8, at 32.
[15] *See, generally*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); *see, e.g.* Ed Felton, *Does Hashing Make Data 'Anonymous'?"* TECH@FTC (Apr. 22, 2012), https://techatftc.wordpress.com/2012/04/22/does-hashing-make-data-anonymous/; EPIC, *Online Tracking and Behavioral Profiling*, http://epic.org/privacy/consumer/online_tracking_and_behavioral.html (last visited June 26, 2012).
[16] *See* Ohm, *supra* note 15, at 1721.

Mobile carriers also make consumer data available to law enforcement officials. Under the "third party doctrine" of criminal procedure, which provides that an individual has no expectation of privacy in information voluntarily conveyed to a third party, mobile carriers have made ordinarily private information accessible to law enforcement officials.[17] The law has long tolerated cooperation between telephone service providers and the government, most notably in *Smith v. Maryland* (holding that the police could access suspect's telephone records because they were "exposed" to the suspect's telephone service provider).[18] In the age of smartphones, however, the universe of information now available to law enforcement through the third party doctrine is vastly expanded and far more personal. In some jurisdictions, including the Fifth and First Circuits, law enforcement officials have gained access to historical cell site data, consisting of location information collected over many months, without a showing of reasonable suspicion.[19]

Recently, in response to recent letters from Congressman Ed Markey (D-MA), nine mobile wireless carriers have provided detailed reports of law enforcement requests for user cell phone records.[20] These requests come from agencies--across all levels of government--seeking text messages, caller locations, and other information in the course of investigations. The reports show that companies turn over thousands of records a day in response to subpoenas, court orders, police emergencies, and other requests.[21] The volume of requests has increased as much as 16

[17] *See* EPIC, Brief of Amicus Curiae Urging Affirmance, In re: Applications of the United States of American Historical Cell-Site Data, No. 20884 (5th Cir. Mar. 16, 2012).
[18] *See* Smith v. Maryland, 442 U.S. 738 (1979).
[19] *See* EPIC, Brief of Amicus Curiae Urging Affirmance, In re: Applications of the United States of American Historical Cell-Site Data, at 8; In Re Application of the United States of Amer. for an Order Pursuant to Title 18, United States Code, Section 2703(D) to Disclose Subscriber Information and Cell Site Information, --- F. Supp. 2d ----, 2012 WL 989638 (D. Mass. 2012).
[20] Press Release, Rep. Edward Markey, Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers (Jul. 13, 2012), http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers.
[21] *Id.*

percent for some companies over the last five years, and some carriers have rejected as many as 15 percent of all requests that they found legally questionable or unjustified.[22]

Finally, loss of consumer privacy facilitates discrimination in both the targeted advertising and law enforcement contexts. In retail, price discrimination on the basis of consumer profiles is already common. For example, Orbitz shows Mac users more expensive hotels than PC users, based on findings that "Mac users on average spend $20 to $30 more a night on hotels than their PC counterparts."[23] Based on stereotypes about values, lifestyle, and purchasing habits, American Express boxed anonymized consumers into categories such as "Blue Blood Estates," "Young Literati," and "Shotguns and Pickups" that ostensibly represented psychological characteristics.[24] The labels determined what advertisements and deals the consumers saw, but the consumers had no recourse to challenge the category in which they had been placed. The surveillance necessary to categorize and profile consumers interferes with privacy's value in promoting autonomy: "A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and serves vital individual and collection ends."[25]

Consumers are concerned about the use of their data,[26] but they frequently do not understand the extent to which their data is collected and shared.[27] Cellular devices are so

---

[22] *Id.*

[23] Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL STREET JOURNAL (June 26, 2012), http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html; *see also* BROOKINGS INSTITUTE, FROM POVERTY, OPPORTUNITY: PUTTING THE MARKET TO WORK FOR LOWER INCOME FAMILIES 6 (2006) ("Lower income consumers are generally much less likely than other consumers to compare prices before buying goods and services, making them more susceptible to bad deals.")

[24] Solove, *supra* note 8, at 18-19, 46.

[25] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

[26] *See, e.g.* NielsonWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), *available at* http://blog.nielsen.com/ nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-w hen-it-comes-to-location/; Cellphones and Privacy, N.Y. TIMES, Feb. 11, 2010, *available at http://www.nytimes.com/2010/02/12/opinion/12fri3.html?_r=*; Aleecia M. McDonald and Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Privacy Practices*, Proceedings of the 9th

complex that the average American does not understand how they work or what types of information they are capable of collecting, much less how long that information is stored by mobile carriers.[28] Moreover, even informed users are deprived by carriers of meaningful choice in regard to the collection, storage, and use of their data. For example, Verizon requires consumers to forgo services if those consumers want to prevent the collection of their data,[29] and Sprint subjects consumer information to the privacy policies of third-party purchasers of that information.[30] All four carriers reserve the right to transfer consumers' personal information to third parties as a business asset during corporate business transactions (including acquisition) or bankruptcy.[31] These practices may eventually have a chilling effect on consumer behavior as consumers become more aware of objectionable uses of their data.[32] Consumers should not have to choose between the competing necessities of mobile service and privacy.[33]

II. The Consumer Privacy Bill of Rights

Building on the recommendations of a Green Paper on Privacy and Innovation released by the Department of Commerce's Internet Policy Task Force in December 2010, the

---

Annual ACM Workshop on Privacy in the Electronic Society (WPES) (2010); Stephanie Clifford, *Concern Rises Over Behavioral Targeting and Ads*, N.Y. Times, Mar. 15, 2009, *available at* http://www.nytimes.com/2009/03/16/technology/internet/16privacy.html.

[27] White House, CPBR, at 12, 13 (citing Aleecia M. McDonald and Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Privacy Practices*, Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society (WPES) (2010).

[28] *See id.*

[29] *Privacy Policy Summary*, VERIZON, ttps://www22.verizon.com/about/privacy/ (last visited Jul. 10, 2012).

[30] *Privacy Policy*, SPRINT, https://www.sprint.com/legal/privacy.html (last visited Jul. 10, 2012).

[31] *See* , *e.g*. *Privacy Policy: Highlights*, T-MOBILE, https://www.t-mobile.com/company/website/privacypolicy.aspx (last visited Jul. 10, 2012) ("We may disclose personal information as part of a corporate business transaction, such as a merger or acquisition, joint venture, corporate reorganization, financing, or sale of company assets, or in the unlikely event of insolvency, bankruptcy, or receivership, in which personal information could be transferred to third-parties as a business asset in the transaction.").

[32] Jay Stanely, *The Potential Chilling Effects of Big Data*, ACLU BLOG (Apr. 30, 2012), http://www.aclu.org/blog/technology-and-liberty/potential-chilling-effects-big-data.

[33] The Federal Trade Commission expressed concern over "take-it-or-leave-it" choice for important products or services when consumers have few choices. *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 50-52 (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf [hereafter "FTC"]. It is EPIC's position that mobile telephones are so central to American society that cellular service represents such a service.

Administration released Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy.[34] The report contains a Consumer Privacy Bill of Rights with the following principles:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Security: Consumers have a right to secure and responsible handling of personal data.
- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[35]

The Consumer Privacy Bill of Rights discusses several high-profile privacy issues, including online advertising, data brokers, and children's privacy. The report encourages online advertising companies to "refrain from collecting, using, or disclosing personal data that may be used to make decisions regarding employment, credit, and insurance eligibility" and cited a "Do Not Track" mechanism as an example of a beneficial privacy-enhancing technology.[36] The report calls on data brokers to "seek innovative ways to provide consumers with effective Individual

[34] White House, CPBR.
[35] *Id*. at 1.
[36] *Id*. at 12.

Control."[37] Finally, the report notes that "the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults."[38]

III. The CPBR Provides a Framework Around Which the Commission Should Develop Fair Information Practices

A. The Commission Should Require Carriers to Give Consumers Individual Control Over Information

Regulation that gives consumers control over the collection and dissemination of their data at multiple stages protects privacy by empowering consumers to safeguard their own information. Companies should offer consumers meaningful choices about the collection, storage, and disclosure of consumer data.

First, the FCC should require mobile carriers to give consumers a range of choices about the collection and retention of consumer data before or at the time of collection.[39] Carriers can facilitate consumer choice by implementing available technologies and providing concise, easily understandable notice.[40] By requiring consent before or at the time of collection, the FCC can ensure that consumers fully understand the specific type of data the carrier is asking permission to collect and use before the carrier has access to that data.[41] This approach is more efficient and protective of privacy than the current opt-out system because many consumers do not have the time or patience to read through lengthy privacy policies after the carrier has already begun collecting data.

---

[37] *Id.* at 13.
[38] *Id.* at 15.
[39] FTC at 48 (recommending that companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data).
[40] White House, CPBR at 12.
[41] FTC at 50 ("In most cases, providing choice before or at the time of collection will be necessary to gain consumers' attention and ensure that the choice presented is meaningful and relevant.").

The FCC should also require carriers to obtain, at the time of collection, consent to share a consumer's data with third parties. In March 2012, the Federal Trade Commission recommended that companies obtain the express consent of consumers to share their information with unaffiliated downstream users because of the privacy concerns this practice raises.[42] Consumers that approve of the carrier's collection and use of data may nonetheless believe they have a reasonable expectation of privacy in their data with respect to third parties.[43] Mobile phone users should be able to distinguish between use by the carrier and use by downstream companies. New technologies that protect consumer choice in this regard include the "Do Not Track" mechanism, which allows consumers to prevent third parties from receiving their data.[44] The FCC should require mobile carriers to provide more granular control over consumer data and disclosure than current exists in order to respond to the fact that consumers do not regard all information within those categories as equally sensitive,[45] nor all third party users as equally protective of their privacy.

B. The Commission Should Require Carriers to Respect the Context in which Data Collection Occurs

To effectuate individual control, carriers must respect the context in which it provides services to the consumer. As Professor Helen Nissenbaum has written, "What people care about it not simply *restricting* the flow of information but ensuring that it flows *appropriately* . . . ."[46] The principle of respect for context recognizes that there may be beneficial uses to consumer

[42] FTC at 42.
[43] *Id.*
[44] White House, CPBR at 12.
[45] *See* FTC at 61 ("[W]hether a particular piece of data is sensitive may lie in the 'eye of the beholder' and may depend on a nmber of subjective considerations.").
[46] HELEN FAY NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2009).

data of which the consumer approves, such as use of consumer data to improve service. [47] Respect for context entails requiring carriers to use information for nothing more than the purposes that the consumer has approved. Data should not be used in ways that were not anticipated by the consumer at the time of collection. For example, a consumer that implicitly or explicitly consents to the use of his information by the carrier for the purposes of improving cellular services may have misgivings about the use of his consumer data by third parties or may not understand that third parties are using the data.

Specifically, the FCC should require companies to (1) notify customers of the purpose for which they are collecting data and (2) limit the use of the data to those stated purposes. The principle of respect for context "distinguishes personal data uses on the basis of how closely they relate to the purposes for which consumers use a service . . . ."[48] Carriers should not use data in a way that is inconsistent with the reasons stated at the time of collection.[49] For example, Verizon's privacy policy states that it collects locational data from consumers' phones in order to provide better service.[50] Requirements that incorporated respect for context would prohibit Verizon from conveying locational data to third party data aggregators absent consumers' consent because Verizon has not disclosed this possible use to consumers before or at the time of collection. Consumers should be able to opt-out of uses of their data that are inconsistent with the purposes for which they supplied the data.

The White House and the FTC have already suggested contexts in which consent to data use and collection may be inferred and in which express consent is necessary to protect

[47] White House, CPBR at 17 ("[A]nalyzing how consumers use a service in order to improve it, preventing fraud, complying with law enforcement orders and other legal obligations, and protecting intellectual property all have been basic elements of doing business and meeting companies' legal obligations.").
[48] *Id.* at 16-17.
[49] *Id.*
[50] *Privacy Policy Summary*, *supra* note 26.

consumers' expectations of privacy. Data may be collected, used, and even disclosed if the purpose for which the data will be used is necessary to achieving the objective that the consumer specifically requested by enrolling in the carrier's service.[51] This implied consent is limited to those instances in which there is a common understanding of service. Carriers could be permitted to collect, store, analyze, and share information without express consumer consent in order to conduct or improve cellular service to the consumer.[52] Similarly, carriers may use consumers' information to market their own products, as this use is "consistent with the consumer's relationship with the business . . . ."[53] Circumstances where express consent was necessary included sharing information with unaffiliated third parties and affiliated third parties where the affiliation is not easily deduced by the consumer. Additionally, the FTC recommended that companies obtain the affirmative express consent of consumers to collect and store sensitive information, such health data, Social Security numbers, and precise, individualized locational data.[54]

C. The Commission Should Require Carriers to Provide Transparency in their Data Practices

The Commission should require mobile carriers to take several steps to ensure transparency. First, providers should be required to provide details on disclosures of personal data with third parties.[55] Second, uses of personal data that are inconsistent with the context of a transaction must be given more prominent disclosure so that consumers can easily identify and

[51] White House, CPBR at 17.
[52] *Id.* at 18.
[53] FTC at 40.
[54] FTC at 58-60; *see also* White House, CPBR at 18.
[55] White House, CPBR at 15.

compare privacy practices.[56] Third, providers should be required to consider mobile phone characteristics, including small screens and privacy risks, when providing notice to consumers.[57]

The Commission should require carriers to inform each customer of the identity of every affiliate, agent, or entity to whom the customer's personal information has been disclosed. This notice could be included with monthly billing statements, should be written clearly and conspicuously, and should alert the customer to any change in the list of companies who has received his or her information. Such a system could be quite similar to that established under California law.[58] Section 1798.83 of the California Civil Code requires businesses that have disclosed personal information to third parties, under certain circumstances, to provide consumers with information on what personal information they disclosed and the names and addresses of all the third parties.[59]

Privacy notices are often written in complex language that customers have neither the patience nor ability to read, and are concealed amongst less important "junk mail" notices from the same source.[60] The Commission should require providers to provide clear, comprehensive, and easily understandable information to consumers that is aimed at a broad audience and, where appropriate, age-adapted. This information should contain details on personal data collection, use, disclosure, and retention.

D. The Commission Should Require Carriers to Give Consumers Access to Stored Personal Information

The Commission should require mobile wireless service providers to provide reasonable access to personal data stored about them, as well as an easily navigable mechanism to correct

[56] *Id.* at 14.
[57] *Id.*
[58] *See* Calif. Civ. Code § 1798.83; Calif. Pub. Util. Code § 2891 (b).
[59] *Id.*
[60] Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, PRIVACY RIGHTS CLEARINGHOUSE (July 2001), http://www.privacyrights.org/ar/GLB-Reading.htm.

inaccurate information and request the removal of data. Providers should also be required to protect personal data stored on mobile phones.

Stored personal data should be at least as accessible to the consumer as it is to third-party business partners. The right to access increases awareness by giving users the ability to see the full extent of the data collected about them by a company. The right to access increases users' control by placing the locus of ownership closer to the user, who gains the ability to inspect data and take steps to correct orders.

In addition to ensuring consumers have access to personal data collected by mobile providers, the Commission should require companies to implement safeguards that protect the privacy of customer information stored in mobile communications devices. Vast amounts of personal information are stored on cell phones, and in many cases it can be very difficult to remove.[61] Unless consumers are given the ability to permanently delete that information, it can be compromised when a phone is refurbished, lost, or stolen. Software can be cheaply purchased that allows purchasers of refurbished or used cell phones to retrieve personal information from them.[62] In a recent test, one analyst found many resold devices still contained personal data.[63]

The Commission should require carriers to configure wireless devices so consumers can easily and permanently delete personal information, as well as permanently erase all information on cell phones before refurbishing and reselling them. In addition, carriers should be required to provide a service that would delete personal information remotely. This would provide a mechanism for data security in the event of a lost or stolen phone, as well as providing mobile phone users with protection against improper seizures if police acquire their phones. Lastly,

[61] *See* Deborah Netburn, *How to Protect Personal Data on Devices You Plan to Sell*, L.A. TIMES (Mar. 29, 2012), http://articles.latimes.com/2012/mar/29/business/la-fi-tech-savvy-protecting-identity-20120329.
[62] Ted Bridis, *Secrets linger on old cell phones*, HOUSTON CHRONICLE, Aug. 31, 2006, at A1.
[63] Michael Estrin, *Don't Be Stupid With an Unwanted Smartphone*, FOX BUSINESS (June 26, 2012), http://www.foxbusiness.com/personal-finance/2012/06/26/dont-be-stupid-with-unwanted-smartphone/.

carriers should include in the software installed on mobile phone devices an easy way for customers to permanently delete personal information.

E. The Commission Should Require Carriers to Protect the Security of Personal Information

The Commission should develop security requirements for mobile carriers based on those set forth in the CPBR. Carriers should be required to "assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure."[64] Additionally, EPIC recommends that carriers provide customers with prudent notification of security breaches and encrypt stored CPNI in order to reduce the risk of harm to consumers.

The FCC should implement a mandatory scheme for notifying consumers in the event of a security breach. EPIC has previously encouraged the FCC to adopt the stance that carriers have a duty to ensure a timely disclosure to consumers when a breach has occurred.[65] Timely notification of a security breach is even more important now that carriers may maintain specific user location data. When a breach of such information occurs it is the consumer that is best able to minimize or prevent harm, thus disclosure must be mandatory. Additionally, economic incentives to promote privacy are only effective if the public is aware of security breaches and can make decisions about carriers accordingly. EPIC reiterates that public breach disclosure is the best way to make sure these incentives are successful.

All CPNI should be encrypted in order to safeguard confidentiality and protect against security breaches. Precisely because encryption may be costly to carriers,[66] the FCC must

[64] *Id.*
[65] *See* Further Notice of Proposed Rulemaking: Customer Proprietary Network Information, *Comments of the Consumer Coalition* (Jul. 9, 2007) *available at* https://epic.org/privacy/wireless/epic_comments.pdf.
[66] Qwest, Comments before the FCC on Implementation of the Telecommunications Act of 1996, Apr. 28, 2006, CC Docket No. 96-115, at 10.

mandate it in order to shield consumers' private information. A number of carriers employ encryption protocols for transmission of information when customers view their data online.[67] Broadening such protocols is a reasonable extension of carriers' existing practices and should be ensured by the FCC. Requiring encryption of all CPNI data also provides carriers with the economic incentive to collect only as much data as needed. The added costs of encrypting all data will put in place economic incentives to retain a lesser amount of CPNI.

In order to hold carriers accountable for the security of consumers' information the FCC must set out a clear definition for "reasonable safeguards" related to security as well as standard practice and reporting for the assessment of privacy and security risks. Federal regulators in the banking industry have given additional guidance to companies on the definition of reasonable security[68] and the FCC should do the same with carriers.

F. The Commission Should Require Carriers to Limit the Collection and Retention of Personal Information

The Commission should adopt data minimization requirements based on those described by the CPBR. Carriers should "collect only as much personal data as they need to accomplish purposes specified under the respect for context principle," and "should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise."[69]

Reduction and regulation of the amount of data collected and the period that data is retained will greatly reduce the amount of data vulnerable to those who would misuse it, both

[67] *See Sprint Privacy Policy, Network and Information Security*, SPRINT, http://www.sprint.com/legal/sprint_privacy.html#network (last visited Jul. 10, 2012); *AT&T Privacy Notice, How We Protect Your Information*, AT&T, http://www.att.com/gen/privacy-policy?pid=7666#108 (last visited Jul. 10, 2012); *Qwest Online Privacy Policy*, QWEST, http://www.qwest.com/privacy (last visited Jul. 10, 2012); *Internet Privacy Policy*, VERIZON, http://www22.verizon.com/privacy (last visited Jul. 10, 2012).

[68] *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL ("FFIEC"), INFORMATION SOCIETY IT EXAMINATION HANDBOOK (2006), *available at* http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.

[69] *Id.*

within and without the carrier. Such reductions are necessary because of the almost-daily occurrence of security breaches. To date over 562 million data records of U.S. residents have been exposed due to security breaches.[70]

The FCC should limit collection of data to accomplishing a business purpose that is clearly specified. The FTC recommended in a March, 2012 report that "companies should limit their data collection to that which is consistent with the context of a particular transaction of the consumer's relationship with the business, or as required or specifically authorized by law."[71] The FCC should adopt a similar policy in order to ensure that carriers limit their collection of consumer data. The FTC report further recommends that when data collection is not done in this manner there should be prominent notice and choice.[72] The FCC should adopt this policy for carriers as well.

In addition to limiting the collection of data it is important that the FCC encourage carriers to have reasonable data retention and disposal policies. EPIC in the past has opposed mandatory statutory data retention[73] and in the same vein EPIC urges to the FCC to ensure that carriers retain CPNI data for the shortest duration possible. The FCC should work to establish a schedule for disposing of retained data after a reasonable time.

IV. Conclusion

To protect the privacy and security of consumers' personal information, EPIC recommends that the Commission require carriers to implement Fair Information Practices similar to those outlined in the CPBR.

---

[70] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, http://www.privacyrights.org/data-breach#CP.
[71] FTC at 26.
[72] *Id.*
[73] *See Hearing on H.R. 1981, the Protecting Children from Internet Pornographers Act of 2011 Before the Subcomm. On Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112 Cong. (2011) (statement of Marc Rotenberg, Executive Director, EPIC; adjunct Professor, Georgetown University Law Center).

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
David Jacobs, EPIC Consumer Protection Fellow
Allegra Funsten, EPIC IPIOP Clerk
Eric Felleman, EPIC IPIOP Clerk
John Sadlik, EPIC IPIOP Clerk
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)

John M. Simpson
Privacy Project Director
Consumer Watchdog
1750 Ocean Park Blvd. ,Suite 200
Santa Monica, CA, 90405
Tel: 310-392-7041
Cell: 310-292-1902