NO. 11-17483

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BENJAMIN JOFFE, et al.,

Plaintiffs-Appellees,

v.

GOOGLE, INC.,

Defendant-Appellant

On Appeal from the United States District Court
for the Northern District of California, Case No. 5:10-MD-2184-JW
Hon. Judge James Ware, U.S. District Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLEES AND URGING AFFIRMANCE

Marc Rotenberg
Counsel of Record
Alan Butler*
David Jacobs*
Electronic Privacy Information Center
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

March 30, 2012

---

* Mr. Butler is currently admitted to practice in the state of California.
* Mr. Jacobs has satisfied the requirements to practice and is pending admission in the State of New York.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

REGULATIONS

OTHER AUTHORITIES

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1]

EPIC routinely participates as *amicus curiae* before the United States Supreme Court, federal circuit courts, and state appellate courts in cases concerning privacy issues, new technologies, and constitutional interests, such as: *FAA v. Cooper*, 132 S. Ct. ____, 2012 WL 1019969 (2012); *United States v. Jones*, 132 S. Ct. 945 (2012); *First Am. v. Edwards*, 610 F.3d 514 (9th Cir. 2010), *cert. granted* 131 S. Ct. 3022 (2011) (No. 10-708); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011); *FCC v. AT&T Inc.*, 131 S. Ct. 1177 (2011); *Doe v. Reed*, 130 S. Ct. 2811 (2010); *Quon v. City of Ontario*, 130 S. Ct. 2619 (2010); *Flores-Figueroa v. United States*, 556 U.S. 646 (2009); *Crawford v. Marion Cnty. Election Bd.*, 553 U.S. 181 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Dep't of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract*

[1] Appellant Google does not consent to the filing of this brief. EPIC has submitted a motion for leave to file contemporaneous with this brief pursuant to Fed. R. App. P. 29(b). In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *IMS Health Inc. v. Sorrell*, 630 F.3d 263 (2d Cir. 2010); *IMS Health v. Ayotte*, 550 F.3d 42 (1st Cir. 2008) *cert. denied,* 129 S. Ct. 2864 (2009); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006); *Gonzales v. Doe*, 449 F.3d 415 (2nd Cir. 2005); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); *Commonwealth v. Connolly*, 913 N.E.2d 356 (Mass. 2009); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a particular interest in ensuring that federal privacy laws protect the users of new communications services. As the central purpose of the Electronic Communications Privacy Act of 1986 ("ECPA") was to update the privacy protections established in the federal Wiretap Act of 1968 so as to ensure the confidentiality of digital communications, EPIC strongly believes that the statute must be construed so as to treat the purposeful intercept of private electronic communications as an unlawful act.

SUMMARY OF THE ARGUMENT

This case involves the intentional interception of electronic communications sent over home Wi-Fi networks. The intercepted data includes personal information and communications – passwords, e-mails, financial records, and other documents – that individuals consider extremely private. The fact that this data was transferred over a wireless network does not change its private nature. Internet users are constantly at risk of cyber attacks and exploits, but they still retain their right in law to communicate privately across computer networks. The Electronic Communications Privacy Act of 1986 ("ECPA") ensures the privacy of these communications, and its protections should not be interpreted in an unfair and inconsistent way. The fact that sophisticated parties may be able to obtain the contents of private communications by intercepting and downloading them does not make those communications "readily accessible to the general public."

Residential Wi-Fi networks enable point-to-point communications between specific devices, such as computers, printers, and Internet routers. These communications are not "broadcast" like traditional radio communications; they are sent from one device to another directly and there is nothing about the typical configuration of a Wi-Fi device to suggest that users expect that their communications between these devices would be "readily accessible to the general public." Consumers intend for their Internet communications to be private, and this

Court should respect their expectations and uphold the purpose and plain language of the ECPA.

ARGUMENT

The Wiretap Act creates a private right of action against any person who "intentionally intercepts . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). However, the Act does not prohibit the interception of any "electronic communication made through an electronic communication system that is *configured* so that such electronic communication is readily accessible to the general public." *Id.* § 2511(2)(g) (emphasis added).

A home Wi-Fi network transmits data using radio waves and thus transmits "electronic communication[s]." *See id.* § 2510(12). Wi-Fi transmissions are not, however, "readily accessible to the general public." The frequency, power, and range of a typical Wi-Fi transmission, as well as the point-to-point nature of the communications, distinguish Wi-Fi fundamentally from the kind of radio communication that Congress considered readily accessible to the general public: a traditional radio broadcast. Furthermore, holding that home Wi-Fi transmissions are readily accessible to the general public, and thus unprotected, would unfairly require users of new communication services to constantly survey the complex and evolving Wi-Fi security landscape and perform technical adjustments to their Wi-Fi settings. This is a burden that the Act does not impose on consumers of

similar technologies, such as wired and cellular Internet communications, and it would be unreasonable to do so here.

For the typical user, a Wi-Fi network transmits the most private types of communications—personal emails, pictures, videos, passwords, banking records, and private documents—within the confines of the home, a space where "privacy expectations are most heightened." *California v. Ciraolo*, 476 U.S. 207, 213 (1986). *See also Kyllo v. United States,* 533 U.S. 27 (2001).[2] This Court should uphold the district court's conclusion that these transmissions are not open to interception and collection merely because very sophisticated companies have the ability to intercept and record this information from a Wi-Fi network.

I. Wi-Fi Networks Enable Private Communications That Are Not Readily Accessible to the General Public

About "one-third of US households" with broadband Internet access have a Wi-Fi network. Wi-Fi Alliance, *The State of Wi-Fi Security* (Jan. 2012).[3] Wi-Fi networks differ from traditional radio broadcasts in several ways, and they should

[2] "While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes -- the prototypical and hence most commonly litigated area of protected privacy -- there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable." *Id*. at 34 (Holding that the use of a thermal imaging device outside the home to capture information about activity inside the home is an impermissible search.).

[3] http://www.wi-fi.org/sites/default/files/uploads/files/wp_State_of_Wi-Fi_Security_20120125.pdf.

not be categorized as "readily accessible to the general public" under the Wiretap Act. Wi-Fi networks transmit radio signals at higher frequencies and lower output power than traditional radio broadcasts, their operating range is comparatively limited. These networks are used by consumers to connect various household devices to each other and to the Internet. So for example, a typical user might install a Wi-Fi device in a home to connect a printer in an office with a desktop computer in a kitchen, a portable laptop, and a wireline Internet connection that leads outside the home.

Wi-Fi networks are not intended to broadcast communications to a vast, unknown, public audience. These networks are designed to deliver data from *point to point* along wireless and wired channels. Unlike a traditional radio broadcast device, a wireless device must be authenticated to send and receive point-to-point communications. Moreover, those who can overhear radio communications do not routinely record the contents of a radio broadcast. Accordingly, there is a sharp distinction between intercepting and recording the communications that travel across a Wi-Fi network and receiving the content of a traditional radio broadcast.

A. The Difference Between Wi-Fi Networks and Radio Broadcast

Wi-Fi networks transmit signals between Wi-Fi connected devices and access points (also known as routers) using radio waves.[4] Home Wi-Fi networks transmit signals in two FCC-unlicensed frequency bands: 2400 MHz and 5000 MHz. *See* 47 C.F.R. §§ 15.247, 15.401-407; *see also* Fed. Commc'n Comm'n, Spectrum Policy Task Force, *Report of the Unlicensed Devices and Experimental Licenses Working Group* 8, 10 (2002) (listing the unlicensed frequency ranges as 902-928 MHz, 2400-2483.5 MHz, 5150-5350 MHz, and 5725-5850 MHz).[5] Whether a Wireless Local Area Networks ("WLAN") device broadcasts in the 2400 MHz band, the 5000 MHz band, or both, depends upon which of the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 operating standards the

[4] The electromagnetic spectrum is "the full range of frequencies, from radio waves to gamma rays, that characterizes light." NASA, *Imagine the Universe! Dictionary*, http://imagine.gsfc.nasa.gov/docs/dict_ei.html#em_waves (last updated Dec. 30, 2004). Radio waves, the form of electromagnetic radiation with the lowest energy, occupy of the portion of the electromagnetic spectrum with frequencies between .01 Megahertz (MHz) and 300,000 MHz. Nat'l Radio Astronomy Observatory, *NRAO Radio Astronomy Glossary,* http://www.nrao.edu/imagegallery/glossary.shtml#r (last updated Nov. 21, 2007). In the United States, the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) allocate the radio spectrum frequencies between .009 MHz and 275,000 MHz. Fed. Commc'n Comm'n, *Radio Spectrum Allocation*, http://www.fcc.gov/encyclopedia/radio-spectrum-allocation (last updated Jan. 5, 2012).

[5] *Available at* http://transition.fcc.gov/sptf/files/E&UWGFinalReport.pdf.

device follows.[6] The current base standard is 802.11-2007[7] and it includes five amendments that govern international compliance and spectrum use. *See* Guido R. Hiertz et al., *The IEEE 802.11 Universe*, IEEE Commc'n Magazine, Jan. 2010, at 62, 64.[8] The 801.11 standard defines medium access control ("MAC") and physical layer specifications. *See* IEEE Std. 802.11-2007, *supra*. The most recent amendment, 802.11n, allows for operation alternatively or concurrently in both the 2400 and 5000 MHz bands. *See* IEEE Computer Soc'y, *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 5: Enhancements for Higher Throughput* (2009) [hereinafter *IEEE Std. 802.11n-2009*].[9] Although the FCC does not require a

---

[6] The 802.11 series includes the general-purpose Wi-Fi 802.11a, 802.11b, 802.11g, and 802.11n standards, each of which differs slightly in bandwidth and signal frequency. *See* IEEE Standards Ass'n, *IEEE 802.11: Wireless Local Area Networks (LANs)*, http://standards.ieee.org/about/get/802/802.11.html (last visited Mar. 29, 2012). The 802.11a standard operates in the 5000 MHz band, the 802.11b and 802.11g standards operate in the 2400 MHz band, and the 802.11n standard has the capability of operating alternatively or concurrently in the 2400 and 5000 MHz bands.

[7] *See* IEEE Computer Soc'y, *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* 1 (2007) [hereinafter *IEEE Std. 802.11-2007*].

[8] *Available at* http://titania.ctie.monash.edu/wireless-nets/hiertz2010.pdf.

[9] http://standards.ieee.org/getieee802/download/802.11n-2009.pdf.

license to broadcast at 2400 and 5000 MHz, the agency does limit the peak output power of such devices to 1 watt. *See* 47 C.F.R. § 15.247(b).

Other standards have been designed to provide Wi-Fi communication among devices within a broad geographic range. However, these are not the devices that are deployed by users of home Wi-Fi networks. These devices are explicitly designed to provide broad public access, which is known to the operators who must actively configure them for that purpose. Worldwide Interoperability for Microwave Access (WiMAX) and the 802.16 Wireless Metropolitan Network ("WMAN") standard upon which WiMAX is based are both designed to broadcast over a range of several miles. *See* WiMax Forum, *Resources – Frequently Asked Questions*;[10] IEEE Standards Ass'n, *IEEE 802.16: Broadband Wireless Metropolitan Area Networks (MANs)*.[11] The plaintiffs in this case did not use wireless devices that were designed to enable access to the general public. In fact, any person creating a home wireless network would not use such a device precisely because they would not intend to enable broad public access.

In contrast, traditional radio broadcasts like AM, FM, and Citizens Band (CB) radio, transmit analog signals using different frequencies and power levels. AM radio broadcasts in the 0.535-1.605 MHz range, FM radio broadcasts in the 88

[10] http://www.wimaxforum.org/resources/frequently-asked-questions (last visited Mar. 29, 2012).
[11] http://standards.ieee.org/about/get/802/802.16.html (last visited Mar. 29, 2012).

MHz-108 MHz range, and CB radio broadcasts in the 26.965-27.405 MHz range. *See* U.S. Dep't of Commerce, Nat'l Telecomm. & Info. Admin., *United States Frequency Allocations* (2003);[12] *see also* 47 C.F.R. § 2.106 (describing frequency bands for traditional radio broadcasting: 530-1610 kHz for AM radio; 5.9-26.1 MHz for shortwave radio; 26.965-27.405 MHz for CB radio; 54-88 MHz for TV channels; and 88-108 MHz for FM radio). Traditional radio broadcasts also greatly exceed the 1-watt power limit placed upon Wi-Fi devices. For example, the operating power of FCC-licensed AM radio stations ranges from 250 to 50,000 watts, while the operating power of FCC-licensed FM radio stations ranges from 6000 to 100,000 watts. *See* Fed. Commc'n Comm'n, *Encyclopedia – FM Broadcast Station Classes and Service Contours*;[13] *see also* Fed. Commc'n Comm'n, *Encyclopedia – AM Broadcast Station Classes; Clear, Regional, and Local*.[14]

B. Residential Wi-Fi Networks Are Designed and Used to Enable Internet Connectivity Within the Home

Although both Wi-Fi networks and traditional radio broadcasts transmit information using radio waves, the power and range of each technology affects the degree to which the communications are publicly available. Radio waves attenuate

[12] *Available at* http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf.
[13] http://www.fcc.gov/encyclopedia/fm-broadcast-station-classes-and-service-contours (last visited Mar. 29, 2012).
[14] http://www.fcc.gov/encyclopedia/am-broadcast-station-classes-clear-regional-and-local-channels (last visited Mar. 29, 2012).

with the square of frequency and the square of distance. John A. Stine & David L. Portigal, MITRE Corp., *An Introduction to Spectrum Management* 1-29 (2004). A 400 MHz signal, for example, will be 100 times weaker at the same distance than a 40 MHz signal. *Id.* Thus, lower frequency signals are much better suited for long-distance propagation. The attenuation of a radio signal also depends upon the power (expressed in decibels (dB) or watts) with which it is initially broadcast. For a signal broadcast at any given frequency, the loss of energy increases with distance. Fed Commc'n Comm'n, Pub. Safety & Homeland Sec. Bureau, *Techtopics – Tecy Topic 17: Propagation Characterization*.[15] For example, a 450 MHz signal loses about 14 dB as it travels between 10 and 50 miles from the source. *Id.* A host of additional factors also affect signal loss, such as the presence of physical objects such as buildings or foliage, and the medium of transmission. *Id.*

Traditional radio broadcasts transmit information using relatively high-power, low-frequency signals that degrade less than the low-power, high-frequency signals used by Wi-Fi devices. Thus, AM radio stations can have a service range of up to 100 miles, while individual Wi-Fi access points have a range of 70-300 feet. *See* Fed. Commc'n Comm'n, *Encyclopedia – Why AM Radio Stations Must Reduce*

[15] http://transition.fcc.gov/pshs/techtopics/techtopics17.html (last visited Mar. 29, 2012).

Power, Change Operations, or Cease Broadcasting at Night;[16] *see also* Michael Richardson & Patrick Ryan, *Wi-Max: Opportunity or Hype?*, 4th Ann. Proc. ITERA Conf., 2006.[17]

Consumer use of and attitudes toward Wi-Fi technology is consistent with these limitations on range. Most consumers use Wi-Fi to connect various devices to each other and to the Internet within the home. Wi-Fi Alliance, a non-profit industry association, describes the typical use of a Wi-Fi network:

> Wi-Fi networks allow multiple users to wirelessly access shared resources such as computers, printers, servers and broadband Internet connections. . . . The broadband modem connects the network to the Internet through a service provider (e.g. cable or DSL). . . . Wi-Fi networks can include traditional computer equipment like laptops and printers, but can also include a growing range of consumer electronics including televisions, cameras, gaming consoles, media players and mobile phones.

Wi-Fi Alliance, *Discover and Learn – Simple Home Network* (2012).[18] Not surprisingly, users of home Wi-Fi expect that communications sent over their networks will remain private. A recent survey by the Wi-Fi Alliance found that 97% of users surveyed expected that the data on their devices and networks would

[16] http://www.fcc.gov/encyclopedia/why-am-radio-stations-must-reduce-power-change-operations-or-cease-broadcasting-night (last visited Mar. 29, 2012).
[17] *Available at* http://lms.uni-mb.si/~meolic/ptk-seminarske/wimax.pdf.
[18] http://www.wi-fi.org/discover-and-learn/simple-home-network (last visited Mar. 29, 2012).

be safe and secure. Press Release, Wi-Fi Alliance, *Wi-Fi Security Barometer Reveals Large Gap Between What Users Know and What They Do* (Oct. 5, 2011).[19]

User behavior also reveals a clear distinction between connecting to a Wi-Fi network to gain access to the Internet and intercepting the content of communications being transmitted using a Wi-Fi network. Approximately 32% of Internet users admitted to accessing and using the non-password protected Wi-Fi networks of their neighbors for the purpose of gaining access to the Internet. Press Release, Wi-Fi Alliance, *Make Security a Priority in 2011: Protect Your Personal Data on Wi-Fi Networks* (Feb. 2, 2011).[20] However, there is no indication that a similar percentage of Internet users have the interest, or the technical capability, to intercept and download the Internet communications of others In fact, among those who defend "piggybacking" off of others' Wi-Fi networks, this distinction is used as a justification for the moral permissibility of the practice. *See* Eric Bangeman, *The Ethics of "Stealing" a WiFi Connection*, Ars Technica (Jan. 9, 2008) ("If the WiFi waves come to you and can be accessed *without hacking*, there should be no question that such access is legal and morally OK") (emphasis added).[21]

---

[19] http://www.wi-fi.org/media/press-releases/wi-fi%C2%AE-security-barometer-reveals-large-gap-between-what-users-know-and-what.
[20] http://www.wi-fi.org/media/press-releases/make-security-priority-2011-protect-your-personal-data-wi-fi%C2%AE-networks.
[21] http://arstechnica.com/security/news/2008/01/the-ethics-of-stealing-a-wifi-connection.ars.

Many commercial businesses, particularly those trying to generate walk-in traffic, such as coffee shops, may choose to create a public Wi-Fi hotspot to attract customers. Starbucks, for example, now offers free Wi-Fi to customers. Press Release, Starbucks, *Starbucks Turns on Free Wi-Fi for Customers July 1st* (Jun. 29, 2010).[22] As Starbucks states, this service is aimed at members of the public, namely, customers of Starbucks. *See id.* Yet Wi-Fi hotspots have the same service range limitations as home networks. As with home Wi-Fi networks, users of Wi-Fi hotspots expect privacy in their communications. When accessing the Internet using a public hot spot, only 18 % of users surveyed by Wi-Fi Alliance reported using Virtual Private Network ("VPN") tool.[23] Press Release, Wi-Fi Alliance, *Wi-Fi Security Barometer Reveals Large Gap Between What Users Know and What They Do* (Oct. 5, 2011).[24] Other studies reveal that public Wi-Fi users do not expect that the content of their communications will be intercepted. Predrag Klasnja et al., *When I Am On Wi-Fi I Am Fearless*: *Privacy Concerns & Practices in Everyday Wi-Fi Use*, 27th Proc. Int'l CHI 1993 (2009) (finding that public Wi-Fi users thought that hacking required a great deal of skill and thus was unlikely to

[22] http://news.starbucks.com/article_display.cfm?article_id=411.
[23] A VPN is "[a] network layer encryption scheme that allows remote clients to securely connect to their corporate networks using the Internet." Wi-Fi Alliance, *Glossary – VPN*, http://www.wi-fi.org/knowledge-center/glossary/vpn (last visited Mar. 29, 2012).
[24] http://www.wi-fi.org/media/press-releases/wi-fi%C2%AE-security-barometer-reveals-large-gap-between-what-users-know-and-what.

happen to them).[25] Finally, the distinction between unauthorized access to a Wi-Fi *network* and unauthorized access to the *content* of a Wi-Fi transmission applies in the context of Wi-Fi hotspots as well. Users may access a public Wi-Fi hotspot to gain access to the Internet, but that is not the same as intercepting and downloading the communications of others who use the Wi-Fi hotspot.

In contrast to private Wi-Fi communications, traditional radio broadcasts are accessible to the general public. A traditional FM radio station can reach all potential listeners within 68 kilometers of the transmitter. Fed. Commc'n Comm'n, *Encyclopedia – FM Broadcast Station Classes and Service Contours*. Thus, a radio broadcast in located in Los Angeles could reach 10.9 million people. *See* Arbitron, *Radio Market Rankings: Spring 2012*.[26] Unlike Wi-Fi, there is no distinction between listening to a traditional radio broadcast network and "intercepting" the content of that broadcast. Accessing a radio station that broadcasts at a frequency of 89.3 MHz, such as Southern California Public Radio,[27] necessarily involves intercepting the content of the communications broadcast by that radio station.

C. All Wi-Fi Networks Require Authentication and Wi-Fi Communications Are Necessarily Encoded

Wi-Fi networks enable communications between authorized devices in a digitally encoded format. Unlike traditional radio broadcasts, Wi-Fi networks are

[25] *Available at* http://dl.acm.org/citation.cfm?id=1519004.
[26] http://www.arbitron.com/home/mm001050.asp (last updated Mar. 28, 2012).
[27] http://www.scpr.org/.

designed to deliver data from point to point along wireless and wired channels. The signals sent from Wi-Fi devices are not intended for a broad audience, they are engineered to deliver messages quickly and efficiently to a specific destination. These signals are not "readily accessible to the general public" in any normal interpretation of the phrase.

The IEEE 802.11 standard specifies the basic operating parameters of all Wi-Fi networks. A Wi-Fi network is built around a basic service set ("BSS"), which in its most common deployment involves wireless stations connecting to an Access Point. Feyza Keceli et al., *Achieving Fair TCP Access in the IEEE 802.11 Infrastructure Basic Service Set*, IEEE Int'l Conf. on Commc'n, 2008.[28] In order to join a BSS, a wireless device must synchronize and become associated with the Wi-Fi network. IEEE Std. 802.11-2007, *supra*, at 25. The AP dictates the synchronization parameters that each wireless device adopts in order to join the BSS. *See id.* at 424. The AP controls the authentication of each device on the Wi-Fi network, and allows authenticated devices to associate with and use the network. *See* Intel, *Understanding IEEE* 802.11 Authentication and Association*.[29]

There are two types of authentication in a Wi-Fi network, Open System Authentication and Shared Key Authentication. *See* Jyh-Cheng Chen et al.,

[28] *Available at* http://newport.eecs.uci.edu/~ayanoglu/TCPFairnessICC08.pdf.
[29] http://www.intel.com/support/wireless/wlan/sb/CS-025325.htm (last visited Mar. 27, 2012).

Wireless LAN Security and IEEE 802.11i, IEEE Wireless Commc'n, Feb. 2005, at 27.[30] Regardless of the method used, no wireless device can associate with and communicate over a Wi-Fi network until it has been authenticated. *See* IEEE Std. 802.11-2007, *supra*, at 473, Fig. 11-6. Open System Authentication, which is the default authentication algorithm for devices sold before the 2007 802.11 standard revision, involves a two-step process of (1) identification/request and (2) authentication. *Id.* at 161. Once a device has been authenticated and associated, it can communicate directly with other devices on the LAN and connect to the Internet through the AP. *See Q&A: Wi-fi Explained*, BBC News, Mar. 8, 2006; [31] IEEE Std. 802.11-2007, *supra*, at 35 ("Before a STA is allowed to send a data message via an AP, it shall first become associated with the AP.").

The devices on a Wi-Fi network communicate via encoded messages[32] sent to a specific destination over the wireless channel. *See* IEEE Std. 802.11-2007, *supra*, at 51. The data transferred over Wi-Fi networks is encapsulated into frames at the Logical Link Control sublayer according to the current IEEE International Standard. *See* IEEE Computer Soc'y, *IEEE Standard for Information Technology* -

---

[30] *Available at* http://gicl.cs.drexel.edu/people/regli/Classes/CS680/Papers/802.11/Security/01404570.pdf.

[31] *Available at* http://news.bbc.co.uk/2/hi/technology/4758722.stm (last visited Mar. 27, 2012).

[32] Messages are referred to in the standard as MAC service data units ("MSDUs"). The actual transfer occurs at the PHY layer using radio signals. *See* IEEE Std. 802.11-2007, *supra*, at 1.

Telecommunications and Information Exchange Between Systems - Local and Metropolitan Networks - Specific Requirements: Part 2: Logical Link Control 1 (1998) [*hereinafter* ISO/IEC 8802-2: 1998].[33] The data frames are fragmented according to size and priority, and then transferred over the Wi-Fi network to a specific destination. *See* IEEE Std. 802.11-2007, *supra*, at 55, Fig. 6-1.

At no point during the process of communicating over a Wi-Fi network is the above-mentioned data "reasonably accessible to the general public." In order to communicate with the network, the wireless device must first initiate a connection and associate, and then send encapsulated and encoded data over the network to a specific destination. This data is directly addressed to its destination, and is not intended to be available to other devices. A traditional analog radio device would have no way of distinguishing this data from random noise. The only way this data can be intercepted is with advanced network and computing technology that can re-package fragmented messages in an unknown encoded format. This process is entirely different than the amateur radio broadcast interception at issue in the Wiretap Act exception, 18 U.S.C. § 2511(2)(g)(i) (2011).

[33] *Available at* http://www.signallake.com/publications/1998802.2LogicalLinkControl.pdf.

II. Because Wi-Fi Security Standards Are Subject to Constant Change, the ECPA Protects Both Encrypted and Unencrypted Wi-Fi Communications Against Unlawful Interception

Consumers continue to rely on network technologies that lack adequate security safeguards. Many users have purchased network devices that do not support the most advanced security standards. Other users rely on default configurations that their devices have out of the box. And even sophisticated users acknowledge that their communications devices will be subject to attack. But in none of these scenarios would users reasonably concede that they have made the contents of their Internet communications publicly available to others. In this respect, communications over unencrypted wireless networks are no different from other Internet communications. When users send e-mail, web searches, or enter sensitive personal passwords and financial information over unencrypted connections, they certainly do not intend to broadcast that information to the public. In all cases the users face the risk that an unauthorized party might intercept their communications, and it is in precisely these cases that the Wiretap Act was intended to provide legal protection. Said differently, if these new services provided absolute physical protection for users, there would be no need for additional legal protection. Just as burglary remains a crime whether or not the front door is bolted, privacy laws protect users when the locks are not sufficient.

A. Truly Secure Wi-Fi Encryption Standards Do Not Exist, and Users Cannot Be Expected to Keep Up with the Most Current Interim Standards

Most Wi-Fi equipment ships with the security features disabled. Wi-Fi Alliance, *Discover and Learn – Security*. [34] Most APs are "shipped with a default network name (SSID), and administrative credentials (username and password) to make configuration as simple as possible." *Id.* Many users never create passwords for their Access Points, and those who do often fail to create strong passwords. *See* Press Release, Wi-Fi Alliance, *Wi-Fi Security Barometer Reveals Large Gap Between What Users Know and What They Do* (Oct. 5, 2011) , (finding that "only 59 percent of users have implemented passwords meeting basic criteria for strength and privacy").[35] However, even strong passwords are often insufficient to protect the privacy and security of Wi-Fi communications. In the past, Wi-Fi protections have either failed to protect users or created new vulnerabilities.

To address early Wi-Fi security flaws, the Wired Equivalent Privacy (WEP) standard was ratified by the IEEE in 1999 as part of the 802.11 standard. *See* IEEE Computer Soc'y, *Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and*

[34] http://www.wi-fi.org/discover-and-learn/security (last visited Mar. 29, 2012).
[35] http://www.wi-fi.org/media/press-releases/wi-fi%C2%AE-security-barometer-reveals-large-gap-between-what-users-know-and-what.

Physical Layer (PHY) Specifications 1 (1999) [hereinafter *IEEE Std. 802.11-1999*].[36] WEP was designed to encrypt communications transmitted on wireless networks to protect their content from interception by unauthorized users. Rajiv C. Shah & Jay P. Kesan, *Analyzing Information Technology & Societal Interactions: A Policy Focused Theoretical Framework* 28 (2007) (Ill. Pub. Law Research Paper No. 07-12).[37] Almost immediately, however, fatal vulnerabilities in the security of the WEP standard were discovered. *See* Nikita Borisov, Ian Goldberg, & David Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11*, 7th Int'l Conf. on Mobile Computing & Networking (2001); *see also* Jessey Walker, *Unsafe at Any Key Size: An Analysis of the WEP Encapsulation* (IEEE 802.11 Committee No. 362, 2000) ("In particular, as currently defined, WEP's usage of encryption is a fundamentally unsound construction; the WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4.");[38] Guillaume

[36] *Available at* http://www.cs.uiuc.edu/homes/haiyun/cs598hl/papers/802.11-1999.pdf.
[37] *Available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1028129.
[38] *Available at* https://mentor.ieee.org/802.11/documents?n=2&o=6a0d1d2d3d4a5a7d8a9a&is_year=2000.

Lehembre, *Wi-Fi Security – WEP, WPA and WPA2*, 1 Hakin9 (2006) (listing four methods of attacking WEP-protected networks).[39]

The vulnerabilities in the WEP standard caused the Wi-Fi Alliance to develop an interim standard, Wi-Fi Protected Access (WPA). *See* Wi-Fi Alliance, *WPA Deployment Guidelines for Public Access Wi-Fi Networks* 8 (2004).[40] In 2005, the IEEE developed WPA2, a revised WPA standard. *See* David Halasz, *IEEE 802.11i and Wireless Security*, EE Times (Aug. 25, 2004).[41] WPA2 implements the National Institute of Standards and Technology (NIST)-recommended Advanced Encryption Standard (AES) algorithm. *See* IP Cores, *802.11i AES Core* (Apr. 2005).[42] Currently, the Wi-Fi Alliance recommends WPA2 encryption for all Wi-Fi users. *See* Wi-Fi Alliance, *Knowledge Center – FAQ* (recommending that users change the default usernames and passwords on their networks and "enable strong encryption for your network: WPA2 security with AES").[43] Nevertheless, flaws have been revealed in WPA2 encryption. Wi-Fi Protected Setup, a feature offered by the Wi-Fi Alliance that is enabled by default

---

[39] *Available at* http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf.
[40] http://ftp.3gpp2.org/TSGX/Working/2005/2005-01/TSG-X-2005-01-Vancouver/Opening_Plenary/X00-20050110-022%20WiFi%20Alliance%20re%20Public%20Access%20WiFi/22a%20WPA_for_Public_Access_Final.pdf.
[41] http://eetimes.com/discussion/other/4025006/IEEE-802-11i-and-wireless-security.
[42] http://www.ipcores.com/images/wpa2.pdf.
[43] http://www.wi-fi.org/knowledge-center/faq (last accessed Mar. 29, 2012).

on most devices and was designed to simplify the process of securing a home Wi-Fi network, contain a recently discovered security flaw that could allow an attacker to gain unauthorized access to a home network. *See* Stefan Viehböck, *Brute Forcing Wi-Fi Protected Setup* (Dec. 26, 2011) (unpublished manuscript).[44] The flaw leaves users vulnerable to an attack that can determine a user's PIN in less than 4 hours. *Id.* at 9. As a result, the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) warned that

> an attacker within range of the wireless access point may be able to brute force the [Wi-Fi Protected Setup] PIN and retrieve the password for the wireless network, change the configuration of the access point, or cause a denial of service. . . . The lack of a proper lock out policy after a certain number of failed attempts to guess the PIN on some wireless routers makes this brute force attack that much more feasible.

US-CERT, *Vulnerability Note VU#723755: WiFi Protected Setup (WPS) PIN Brute Force Vulnerability* (Dec. 27, 2011).[45] US-CERT concluded that "[w]e are currently unaware of a practical solution to this problem." *Id.* Tactical Network Solutions is now selling Reaver, a WPA attack tool that exploits this security flaw in Wi-Fi Protected Setup. *See* Tactical Network Solutions, *Products – Reaver Pro*.[46] The company claims that "Reaver is able to extract the WPA [Pre-Shared Key] from the access point within 4 - 10 hours and roughly 95% of modern consumer-grade access points ship with [Wi-Fi Protected Setup] enabled by

[44] https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.
[45] http://www.kb.cert.org/vuls/id/723755 (last revised Feb. 09, 2012).
[46] http://www.tacnetsol.com/products/ (last visited Mar. 29, 2012).

default." *Id.* Once on the network, it is "simple" for a computer criminal to use free programs such as Firesheep to intercept the content of the communications being sent over that network.[47] Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, NY Times, Feb. 16, 2011, at B8.[48]

B. Many Older Devices Do Not Support Current Security Standards, But Communications Over These Devices Are Still Private

Many home networking devices have open or insecure default configurations, and devices that were deployed before 2007 are typically not compatible with the Robust Network Security Architecture described in the IEEE 802.11-2007. The ECPA legal protections should not rise or fall based on the level of security established in a particular Wi-Fi network. Regardless of the strength of the authentication method used, a Wi-Fi network enables private communications between specific devices on the network. *See supra* Part I.B. Wi-Fi users should not be denied a legal remedy to the interception of their data because they did not purchase or configure the most secure network technology.

The RSA, an American computer and network security firm, published a survey of wireless security used in New York City Wi-Fi networks in 2008. *See*

---

[47] It is important to note that even though the instructions necessary to complete this hack are widely available on the Internet, it still requires sophisticated software and hardware to implement. As with lock-pick kits, or instructions for stealing a car, the existence of the tool should not legitimize the unlawful behavior.

[48] https://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html?_r=1.

RSA: The Security Division of EMC, *The Wireless Security Survey of New York City* (4th ed. 2008).[49] This survey found that slightly more than 50% of wireless networks employed unsecure encryption standards. *Id.* at 4. For some users the lower level of security may come from a lack of understanding of the technology or incompatible hardware. However, even security experts may prefer to operate networks with no password protections for a variety of reasons. *See* Bruce Schneier, *Steal This Wi-Fi*, Wired, Jan. 10, 2010.[50] These reasons include convenience, enabling easy Internet access for others, and a recognition that it is more important to secure your device itself than to secure network access. *Id.* For other users, maintaining adequate security standards is simply not possible. Users might choose to secure their networks using MAC filtering or some other non-encrypted method. *See* Wi-Fi Alliance, *Knowledge Base – Articles – MAC Filtering*.[51] According to the Wi-Fi Alliance certification database, only 37% of currently certified devices are compatible with strong encryption standards. *See* Wi-Fi Alliance, *Certified Products*.[52]

---

[49] http://www.rsa.com/solutions/wireless/survey/WLANNY_WP_1008.pdf.
[50] *Available at* http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0110.
[51] http://www.wi-fi.org/knowledge-center/articles/mac-filtering-media-access-control (last visited Mar. 30, 2012).
[52] http://certifications.wi-fi.org/search_products.php? (last visited Mar. 17, 2012).

C. Unencrypted Communications Sent Over Wi-Fi Networks Are No More "Readily Accessible to The General Public" Than Those Sent Over Unencrypted Wired Networks

The Open Authentication Standards used by Wi-Fi networks are no less secure than Internet communications in general. Any data sent over the Internet will necessarily pass through multiple servers and network devices en route to its destination. These devices can easily read unencrypted data packets as they pass through the network. Any e-mail sent over an unencrypted channel can be easily intercepted and read; yet courts have not held that such communications are "readily accessible to the public." The interception of electronic communications should not be deemed legal simply because the user did not employ best security practices.

The technology used to read the contents of Internet communications, 'packet sniffing technology,' is "one of the fundamental tools used to monitor and intercept data over a network." Christopher Jones, *Internet Hacking for Dummies*, Wired, Feb. 20, 1998.[53] These tools can be used to read e-mails, web queries, and even passwords that are sent over unencrypted channels. *See* Internet Security Systems, *Packet Sniffing*.[54] The problem of unencrypted Internet traffic is serious, but there are readily available options to secure most Internet data. *See* Michael E.

[53] *Available at* http://www.wired.com/science/discoveries/news/1998/02/10459.
[54] http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Packet_sniffing/default.htm (last visited Mar. 27, 2012).

Kounavis et al., *Encrypting the Internet*, 40 SIGCOMM 135 (2010).[55] Nevertheless, ECPA protects Internet communications regardless of whether they travels over a wired or wireless, encrypted or unencrypted channel.

D. This Court Should Not Impose a Unique Burden on Wi-Fi Users to Constantly Survey the Complex and Evolving Wi-Fi Security Landscape and Perform Technical Adjustments to Their Wi-Fi Settings

Holding that unsecure Wi-Fi communications are not protected from interception under the Wiretap Act would place unreasonable burdens on Wi-Fi users. First, users would have to purchase new Wi-Fi devices, as many older devices are not compatible with current security standards. *See, supra*, Part II.B. Users would then have to password-protect their AP, ensure that their chosen password is strong, and continually assess the state of Wi-Fi security standards. *See*, *supra*, Part II.A. But even that would not be sufficient, a user would also have to be sure that the *recipient* of their communications was using a similarly secure network configuration. These burdens are not imposed on users of substantially similar communications technologies. Yet the content of unencrypted communications sent through a wired modem is no less subject to interception than that sent over an unencrypted Wi-Fi network.

From the user's perspective, the security of Wi-Fi communications would therefore depend upon a series of arbitrary, complex, and unknown factors. The

[55] *Available at* http://dl.acm.org/citation.cfm?id=1851200.

legal protections should depend upon the private nature of the communications,[56] addressed to a particular device, not on whether a user holds a doctoral degree in Computer Science, or on whether a user accesses the Internet via wired modem, Cell Phone, or wireless network. As the ECPA was specifically enacted in recognition of the development of new communications services for consumer markets, such as electronic mail, it would be contrary to the purpose of the Act to place such a burden on typical users of these services.

CONCLUSION

Amicus respectfully requests this Court to deny Appellant's motion and affirm the decision of the lower court.

---

[56] Even Google has acknowledged the privacy interests associated with the data generated by Wi-Fi networks. The Google Location Server (GLS) uses information gathered from Wi-Fi networks to determine the location of mobile devices. *See* Google, *Location Based Services*, https://support.google.com/maps/bin/answer.py?hl=en&answer=1725632.

In 2011, after investigations by multiple European date protection authorities, Google announced that it would allow users to opt out of having their Wi-Fi network location information included in Google's location server. Peter Fleischer, *Greater Choices for Wireless Access Point Owners*, Google Blog (Nov. 15, 2011), http://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html. Users can opt out by including "_nomap" at the end of their Wi-Fi network name. *Id.* By allowing Wi-Fi users to opt out of its location server, Google confirms that Wi-Fi transmissions involve private data that should be free from surreptitious eavesdropping. If the location and network information of a Wi-Fi network is worthy of protection, then is the content of the emails, passwords, videos, and documents traveling over the network.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 6,190 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14 point Times New Roman style.

Dated: March 30, 2012

/s/ Marc Rotenberg
Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 30th day of March 2012, the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Appellees and Urging Affirmance was electronically filed with the Clerk of the Court, and thereby served upon counsel for the parties *via* electronic delivery. Pursuant to Circuit Rule 31-1, one original and 7 copies were shipped to the Clerk by U.S. Mail, postage prepaid, on March 30, 2012. Two paper copies were shipped to each party by U.S. Mail, postage prepaid, on March 30, 2012.

Dated: March 30, 2012

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140