Can We Sniff Wi-Fi?

Implications of *Joffe v. Google*

Simson L. Garfinkel and Michael McCarrin | Naval Postgraduate School

The US Court of Appeals issued an opinion that Wi-Fi sniffing can violate the US Wiretap Act. If it stands, the ruling may significantly impact computer security education, in which Wi-Fi sniffing is a common student exercise; security practitioners, who sniff for security assessments; and computer security research, where it's common to sniff in order to find vulnerabilities.

On 27 December 2013, the US Court of Appeals for the Ninth Circuit issued an opinion that intercepting data from unencrypted wireless local area networks—Wi-Fi sniffing—can violate the US Wiretap Act (18 USC §2511).[1] The anti-sniffing opinion is another milepost in the long-running battle between Google and privacy advocates over Street View, Google's project to photograph all the planet's streets and neighborhoods and make the data freely accessible over the Internet. It also marks an important step in the evolution of US privacy law and has the potential to place in legal jeopardy scores of computer security students, educators, researchers, and practitioners who routinely sniff Wi-Fi networks.

In this article, we briefly sketch the facts of the case and the Court's reasoning, present the legal history, and discuss the implications for computer security educators and researchers. To keep our analysis manageable, we discuss only US law.

The Facts of the Case

In 2007, Google launched Street View, a layer in Google Maps that lets users see houses, buildings, and street signs. To create this service, Google developed special cameras to capture panoramic imagery, attached those cameras to Google-owned vehicles, and drove the vehicles around the world, filming as they went.[2]

The Street View vehicles also scanned for wireless networks. This kind of network auditing, called *wardriving*,[3] was popularized in 2004 when Marius Milner released NetStumbler, a program that scanned for Wi-Fi access points and recorded their GPS position and security status (open or encrypted). Many of the early "stumblers" were security professionals trying to document the proliferation of unsecured networks; others were mapping enthusiasts who contributed to collaborative, open source mapping projects such as Wigle.net. But some of the stumblers were computer hackers, spammers, and child pornographers searching for open Wi-Fi networks so they could have unattributed Internet access. (The theft of 45 million credit card numbers from TJX, between July 2005 and January 2007, resulted from a network vulnerability found by wardriving.[4])

Google's vehicles made similar wardriving maps. Their purpose was to use Wi-Fi access points to augment GPS for Google's upcoming smartphone. The technique of using Wi-Fi as an alternative to GPS was pioneered by Skyhook Wireless in 2003. The method

 Copublished by the IEEE Computer and Reliability Societies

relies on the fact that each Wi-Fi access point continually sends out a "beacon" with a unique 48-bit MAC address. Because access points rarely move, laptops and cell phones can use a map of access points to determine their position, simply sniffing for all beacons in range and triangulating their position relative to the beacons. (In practice, triangulation is done on a remote server.) Wi-Fi geolocation frequently works better than GPS in cities and indoors because GPS signals are blocked by buildings but Wi-Fi is plentiful.

In 2010, Google conducted a technical review of its Street View program at the behest of privacy regulators in Germany and discovered that the Street View vehicles were recording not only the physical location of Wi-Fi access points but also every 802.11 frame, including user data, from unencrypted networks.[5] In total, approximately 600 Gbytes had been collected in 30 different countries, including the US. A later analysis by the Federal Communications Commission (FCC) found that the collection had been taking place for more than two years and included "names, addresses, telephone numbers, URLs, passwords, e-mail, text messages, medical records, video and audio files, and other information from Internet users in the United States."[6]

Several class-action lawsuits were filed against Google for violating the US Wiretap Act, which was originally passed as part of the Omnibus Crime Control and Safe Streets Act of 1968 and updated by the Electronic Communications Privacy Act (ECPA) of 1986.[7] Those cases were transferred to the Northern District of California and consolidated into a single case, *Joffe v. Google*.[8]

Google filed to have the case dismissed, arguing that capturing this data (at least in the US) was legal under the Wiretap Act, which generally prohibits interception of private wired or wireless communications by third parties but specifically exempts the interception of unencrypted "radio communication … readily accessible to the general public." The trial court rejected Google's motion, finding that Wi-Fi wasn't a radio communication as defined under the act. Google appealed. A three-judge panel at the US Court of Appeals for the Ninth Circuit heard the appeal and denied the motion on 10 September 2013. Google requested an en banc rehearing by the full appellate court, which was also denied. Instead, Judges A. Wallace Tashima, Jay S. Bybee, and William H. Stafford issued an amended decision on 27 December 2013, clearing the way for the trial to proceed.

The FCC also launched an official investigation into the matter, commencing with a Letter of Inquiry to Google on 3 November 2010, requesting additional information. FCC investigators interviewed five Google employees and an employee of the consulting firm that Google had hired to conduct a forensic analysis of the incident. Ultimately, they imposed a US$25,000 fine on Google for obstructing their investigation.

The version of the report that the FCC released was heavily redacted and drew no firm conclusions about Google's intentions; Google later released a somewhat less redacted version in which the FCC claimed that the software on the Street View vehicles "was deliberately written to capture payload data."[9] Still, the FCC decided "not to take enforcement action against Google" for violating the Communications Act (which has provisions similar to the Wiretap Act), because there was no precedent for applying the act to the interception of unencrypted Wi-Fi communications.

Several commentators incorrectly claimed that the FCC concluded Google hadn't violated the Wiretap Act. In fact, in its 13 April 2012 order, the FCC merely declined to make an enforcement action.

The Technology

Introductory texts about network security frequently compare sending information over the Internet without encryption to sending a postcard through the US Postal Service—anyone along the path can access the content without leaving a trace. This is especially true of wireless data, as radio waves radiate in every direction.

Home Wi-Fi access points appear to have various kinds of access control to prevent the signal from reaching unauthorized parties—each network can have its own distinctive name, and many access points allow client filtering by MAC address. However, in practice, every transmitted frame is received by every other Wi-Fi radio that's within range and tuned to the same channel. Once received, computers typically ignore packets intended for other systems. So, although Wi-Fi networks appear to be point-to-point systems, the underlying physics is that of a broadcast network. Indeed, software (like NetStumbler) is widely available to turn ordinary Wi-Fi radios into sophisticated wireless sniffers. Sniffing unprotected networks is a common assignment in many network security classes and an important security technique for finding unauthorized, or *rogue*, access points in an organization. In addition, sniffing is the basis of the Wi-Fi geolocation system used by practically every smartphone, although geolocation requires sniffing only Wi-Fi beacons, not user content.

Even point-to-point wired communications can be intercepted by hackers, criminals, and hostile governments, of course. That's why network communications must be encrypted to ensure their privacy. Encryption doesn't prevent interception, but properly implemented encryption does make the intercepted data useless to anyone who doesn't possess the key. Using encryption is widely regarded as a best practice for all sensitive data sent over the Internet, not just for data sent over Wi-Fi.

There are at least four ways that data sent over Wi-Fi can be encrypted. The wireless network can be encrypted using the Wi-Fi Protected Access (WPA) and WPA2 standards. The IP frames sent over the network can be encrypted using a virtual private network. The TCP layer can be encrypted using Trusted Layer Security (TLS)—for example, if a webpage's URL begins with "https:" it's automatically downloaded using encryption. Finally, the content can be encrypted—for example, a Microsoft Word or Acrobat file downloaded over the Internet can be password protected (both applications implement passwords using 128-bit encryption).

The Law

The Wiretap Act generally prohibits the intentional interception of electronic communications but says that it's not unlawful "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[10] The phrase "readily accessible to the general public" is defined in §2510(16) "with respect to a radio communication" to mean a communication that isn't "scrambled or encrypted" or transmitted using a small set of specialized techniques.

In 1986, Congress amended the Wiretap Act with the ECPA to make it illegal to eavesdrop on cellular telephones, which had been introduced in the US just three years before. The cell phones of the 1980s were analog devices that didn't use encryption, and calls could be readily intercepted with handheld radio scanners. The sale of such scanners stopped in the US following the law's passage, although scanners continued to be sold that could be modified easily to receive cell phone calls, typically by clipping a single wire. In 1993, the *Boston Globe* published an article that called illegal cellular eavesdropping "very, very popular."[11]

Although the ECPA criminalized eavesdropping on analog cell phones, it didn't criminalize eavesdropping on cordless phones. Like cell phones, cordless telephones of that era didn't use encryption; unlike cell phones, it was common to overhear other people's conversations. In the case of *Tyler v. Berodt*, a police department provided recording equipment to Rich and Sandra Berodt so they could record the conversations of their neighbor Scott Tyler, whom the Berodts suspected was conducting drug deals. Tyler found out and sued for wiretapping, but the US Eighth Circuit Court of Appeals ruled the Berodts didn't violate the Wiretap Act because there was no "reasonable expectation" of privacy when using cordless phones.[12] The US Supreme Court declined to hear the case on appeal.[13]

Even though both 1980s cordless phones and today's Wi-Fi devices use the unlicensed radio spectrum, there are important differences. Whereas cordless phones had aspects of a party line, Wi-Fi provides the illusion of privacy, because there's no way to accidentally intercept another person's communications without intentionally running a packet sniffer. On the other hand, because it's common for Wi-Fi users to click their wireless icon and see that there are multiple networks available, one could argue that users have been given notice that the wireless airwaves are a shared resource and subject to monitoring.[14]

Amicus briefs filed last year with the Ninth Circuit took both sides of the issue. For example, the Electronic Privacy Information Center (EPIC) argued that the phrase "radio communication" doesn't include situations "where the user of a communications device does not intend to broadcast communications to the general public," which almost certainly is the case with the Wi-Fi signals that Google captured.[15] EPIC also argued that the ECPA was passed in 1986 specifically to protect unencrypted analog cell phones.

Meanwhile, the Information Technology and Innovation Foundation took the position that the Court's ruling is based on "incorrect factual assumptions about Wi-Fi Technology" and "would place at legal risk standard techniques used every day by information technology professionals and companies around the country."[16]

The Ninth Circuit initially argued that Wi-Fi users have an expectation of privacy because Wi-Fi signals aren't accessible to the general public. This ruling provoked heckles from the tech community and a sarcastic "Privy" nomination for "dubious achievement in privacy law" by Stewart Baker, a former assistant secretary for policy at the US Department of Homeland Security.

The rationale about Wi-Fi not being publicly accessible was removed in the revised opinion, leaving the Court's other argument—that Wi-Fi is *communication by radio*, but not *radio communication*. Drawing examples from the Wiretap Act itself, the Court argued forcefully that the two phrases carry different connotations. Communication by radio, the Court asserted, refers simply to communications that employ radio waves, such as satellite television, paging systems, or Wi-Fi. In contrast, radio communication evokes the more commonsense definition of the phrase—an audio broadcast.

Through this reasoning, the Court concluded that the "ordinary meaning of 'radio communication,' does not include data transmitted over a Wi-Fi network."[10] Furthermore, "Google's proposed definition [of radio] is in tension with how Congress—and virtually everyone else—uses the phrase. In common parlance, watching a television show doesn't entail radio communication, nor does sending an email or viewing a bank statement while connected to a Wi-Fi network."[10]

In the act, the exemption of signals that aren't "scrambled or encrypted" applies only to radio communication. If Wi-Fi isn't radio communication, the exemption doesn't apply. The Court stated that the exemption was created by Congress to protect hobbyists: "Traditional radio services can be easily and mistakenly intercepted by hobbyists. … But 'radio hobbyists' do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks. Lending 'radio communications' a broad definition that encompasses data transmitted on Wi-Fi networks would obliterate Congress's compromise and create absurd applications for the exemption for intercepting unencrypted radio communications."[10]

> **From a public policy perspective, making it illegal to eavesdrop on Wi-Fi networks might paradoxically make networks less secure.**

The Court concluded that it would be poor public policy to apply the exemption to Wi-Fi networks: "It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity."[1]

Should We Sniff?

Although the Court is probably correct that hobbyists don't mistakenly use packet sniffers to intercept payload data, it's quite common for hobbyists, students, and teachers to *intentionally* intercept payload data. Such interceptions demonstrate the ease with which Wi-Fi signals can be captured and, therefore, the importance of encryption. Wireless security courses typically go further still, teaching a variety of passive and active approaches for attacking encrypted networks—not for vicarious thrills, but as an important lesson.

From a security perspective, it shouldn't matter whether or not Wi-Fi networks are encrypted: any sensitive data sent over the Internet should be protected with end-to-end security, such as TLS. So, from a public policy perspective, making it illegal to eavesdrop on Wi-Fi networks might paradoxically make networks less secure, because the legal protection could give network operators a false sense of security.

At the same time, many Internet services don't encrypt all their communication. Clearly, there should be a way to discourage nefarious individuals from collecting information from people using these unencrypted services at public Wi-Fi hotspots, where users have no option to use Wi-Fi encryption. One way to address this is to invoke 18 USC §1029, which criminalizes the possession of 15 or more *access devices* (a term that can include stolen usernames, passwords, and credit card numbers) with intent to defraud.[17] Another approach might be to use copyright or privacy law to prohibit the republishing or disclosure of collected private information.

Months after the Ninth Circuit's revised ruling, the impact is still unclear. Other courts might find the particulars of *Joffe v. Google* extreme and resist applying the ruling to hobbyists or educators that sniff for demonstration purposes. Meanwhile, the ruling is binding only in the Ninth Circuit. In another case, a federal District Court in Illinois explicitly held that sniffing Wi-Fi was legal: "Because data packets sent over unencrypted Wi-Fi networks are readily accessible using the basic equipment described above, the Wiretap Act does not apply here."[18]

Beyond these two contrasting decisions, we could find no other US cases or opinions regarding the legality of passive Wi-Fi sniffing. (This is in contrast to the illegal use of another person's open Wi-Fi, of which there are several cases.) As the FCC's report suggests, no precedent exists for the application of the ECPA to Wi-Fi sniffing.

A Framework for Reasoning about Sniffing

It's likely that the US Supreme Court will eventually make a ruling on this issue. Until then, the legality of wireless sniffing is unclear. Sniffing might be legal depending on a variety of factors, including:

- *The protocol being sniffed*. Most of the rulings have applied solely to Wi-Fi (802.11), but many other wireless protocols operate in the unlicensed radio spectrum, including Bluetooth, ZigBee, and RFID systems. Depending on the final rulings, individuals and organizations wanting to sniff, or prosecute sniffers, might argue that the rulings apply to these other protocols or that these other protocols are fundamentally different and require their own day in court.
- *Whether the sniffed frequency is licensed*. Although Wi-Fi operates in the unlicensed bands, the WiMAX (802.16) system can operate in either the unlicensed or licensed spectrum. Recall that, in the 1980s, it was legal to intercept cordless phones calls that used unlicensed frequencies but illegal to intercept those calls using licensed frequencies. A future ruling that allows sniffing in unlicensed frequencies might not be applicable to licensed bands.
- *The use of encryption and cracking*. *Joffe v. Google* is built on the interception of unencrypted wireless frames. A

future case might clarify distinctions between sniffing encrypted and unencrypted data.

- *Whether the sniffed frames are beacons (and other control frames) or content*. Although *Joffe v. Google* is broadly concerned with sniffing user data such as email messages and Internet searches, the Ninth Circuit Court's ruling could be interpreted to exempt beacons, under the theory that beacons carry no user data, that they are intentionally broadcast to all listeners, and that sniffing beacons is required to provide the underlying service.
- *Whether the entire packet content or just headers are kept*. Many network monitoring tools have provisions for retaining just the packet headers and discarding the rest. Such practices could be explicitly evaluated by a court and found to be either lawful or a violation of the Wiretap Act.
- *Whether those being monitored have given consent*. Many universities require that their network users give consent to being monitored by the university's network staff. Such networks could in turn be used as a living laboratory for the staff to research wireless security and usage patterns, as has been done in the past.
- *The availability of interception hardware and software*. Today, any laptop or smartphone can be turned into a sniffer—this can even be done by malware without the owner's knowledge. But, in the future, consumer hardware might not have sniffing capabilities.

Of paramount importance in all these scenarios is how courts define *Wi-Fi interception*. After all, all Wi-Fi frames are received by any device in range and on the same channel. But the law defines interception more narrowly as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" (18 USC §2510(4)).[10] Thus, a user might avoid breaking the law by discarding the frames quickly or simply by not interpreting them.

Even if this question is settled and a future court finds it legal to intercept unencrypted Wi-Fi under the Wiretap Act, there might be other laws that restrict sniffing. For example, the terms of service for AT&T Wireless Wi-Fi—the service at many Starbucks stores—specifically prohibits running a packet sniffer.[19] Courts have held that failure to comply with such agreements can be a violation of the Computer Fraud and Abuse Act and carry criminal penalties.[20]

> **Much of what we know about the security of wireless systems results from security researchers conducting their own sniffing experiments in the wild.**

Implications for Teaching

Just as educators don't demonstrate the importance of Web security by breaking in to poorly secured commercial websites, it is ethically suspect to demonstrate the importance of Wi-Fi security by collecting a few gigabytes of unencrypted network traffic at a local coffee shop.

Instead, educators and researchers can set up a test network, which affords significantly more control and reproducibility than capturing in the wild. Clearly, nothing in the Court's ruling prohibits educators from eavesdropping on a network that they set up in a lab. Given the Court's broad language, educators might want to take additional measures to avoid accidentally recording packets that happen to be on the same channel as the research network—for example, by creating filters that capture and retain only Wi-Fi packets with specific MAC addresses.

Implications for Security Practitioners

Security professionals might be in the greatest jeopardy with the Court's ruling. Finding rogue Wi-Fi access points is an important part of security auditing. In so doing, practitioners might be at risk of capturing traffic from outside the organization that they're auditing. In principle, this is similar to accidentally performing penetration tests on the wrong computer. However, the risk is higher, because most organizations operate their computers within a specific range of IP addresses, whereas Wi-Fi signals don't respect property lines.

Likewise, many enterprise Wi-Fi access points can now detect and mitigate rogue access points, typically by sniffing for unauthorized Wi-Fi networks, and then sending spoofed disassociation frames. Such activities might not be legal under the Court's ruling.

Implications for Wi-Fi Users in General

For most users, the ability to continue with business as usual depends on the assumption that future courts will interpret the law in such a way that makes allowances for the interception of control frames—an outcome that seems likely, but not yet guaranteed. If sniffing control frames isn't acceptable, then many Wi-Fi services could suddenly become illegal.

Consider what happens when a laptop user clicks the Wi-Fi icon to see a list of the available wireless networks. That list appears because the user's laptop is constantly sniffing the Wi-Fi spectrum for Wi-Fi beacons and processing them. If laptop users can receive Wi-Fi signals only with prior authorization, then the laptop

has no way of creating the list of available networks. Likewise, a strong ruling against sniffing Wi-Fi beacons might make Wi-Fi geolocation schemes illegal.

Implications for Researchers

Much of what we know about the security of wireless systems results from security researchers conducting their own sniffing experiments in the wild. Although many of today's Wi-Fi routers are secured with encryption, there's a growing awareness that other wireless systems being deployed might have little or no built-in security.

If future rulings are tailored to the specifics of Wi-Fi technology—for example, allowing sniffing of beacons but not user content—then researchers working with other wireless systems might find themselves in legal limbo. For example, ZigBee systems are being increasingly deployed, and many of these systems, like early Wi-Fi systems, are open and unencrypted. Is a researcher who drives around with a ZigBee sniffer violating the Wiretap Act? What if the ZigBee data isn't email messages, but pressure readings? What about a graduate student investigating the car-to-car protocol of a future automotive network? Or a high school student examining signals sent between smart meters deployed by her electric utility?

The wireless industry has a poor track record in regard to security in new products. It would be hugely expensive if future courts rule that the only way to research these systems is to set up and operate the equipment in a radio-shielded lab. It's also likely that many security vulnerabilities would remain undiscovered, because many real-world configurations can't be readily replicated.

Our purpose here isn't to claim that the Ninth Circuit's opinion was an error; a list of troubling consequences doesn't refute the Court's logic. Yet here, as elsewhere, the boundaries delimiting public and private data are in flux. Even if the courts were to suddenly resolve the current debate, a resolution of *Joffe v. Google* might be specific to wardriving and offer no long-term guarantee or uniform policy. Furthermore, as the current grounding of Street View vehicles in Germany illustrates, other governments will make their own policies. Even in the US, state and local entities could pass more restrictive laws. Such laws might hold, or they might be preempted by federal statute.

Good questions for security professionals to ask ourselves include the following: What outcome do we desire? Do we want to live in a world where running a Wi-Fi packet sniffer can result in a felony conviction? Do we want there to be no privacy rights to any data that happens to be transmitted over an unencrypted wireless link? Could there be a middle ground—for example, making it legal to intercept packets but illegal to use the information that they contain?

In the absence of widespread consensus, the most prudent course is to avoid sniffing any network equipment that you don't control. Such a cautious approach might be appropriate in an educational environment, but it will have a negative and lasting impact on security research and development. Others will need to decide if such an approach is ultimately in society's best interest. ■

Acknowledgments

We thank Robert Beverly, Andrew Grosso, James Grimmelmann, and Marc Rotenberg for their comments on a previous draft of this article. Simson L. Garfinkel previously volunteered for the Electronic Privacy Information Center, and his spouse is currently employed there. The views expressed in this article are those of the authors and do not reflect the policy of the Naval Postgraduate School, the Department of Defense, or the US government.

References

1. "Opinion, Appeal from the United States District Court for the Northern District of California, No. 11-17483, D.C. No. 5:10-md-02184-JW," Sept. 2013; http://cdn.ca9.uscourts.gov/datastore/general/2013/09/11/11-17483_opinion.pdf.
2. A. Fisher, "Google's Road Map to Global Domination," *New York Times*, 11 Dec. 2013; www.nytimes.com/2013/12/15/magazine/googles-plan-for-global-domination-dont-ask-why-ask-where.html.
3. H. Berghel, "Wireless Infidelity I: War Driving," *Comm. ACM*, vol. 47, no. 9, 2004, pp. 21–26; http://doi.acm.org/10.1145/1015864.1015879.
4. L. Greenemeier, "T.J. Maxx Data Theft Likely Due to Wireless 'Wardriving,'" *InformationWeek*, 9 May 2007; www.informationweek.com/d/d-id/1054964.
5. "WiFi Data Collection: An Update," Google Official blog, 14 May 2010; http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.
6. "DA 12-592: Notice of Apparent Liability for Forfeiture," Federal Communications Commission, 13 Apr. 2012; http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0416/DA-12-592A1.pdf.
7. "18 U.S. Code Chapter 119—Wire and Electronic Communications Interception and Interception of Oral Communications," Legal Information Inst., Cornell Univ.; www.law.cornell.edu/uscode/text/18/part-I/chapter-119.
8. "In Re: Google Inc. Street View Electronic Communications Litigation," Justia Dockets & Filings, 17 Aug. 2010; http://dockets.justia.com/docket/california/candce/5:2010md02184/230845.
9. "DA 12-592: Notice of Apparent Liability for Forfeiture," *Wired*, 13 Apr. 2012; www.wired.com/images_blogs/threatlevel/2012/05/unredactedfccgoog.pdf.

10. "*Joffe v. Google*, No. 11-17483, D.C. No. 5:10-md-02184-JW, Order and Amended Opinion," 27 Dec. 2013; http://cdn.ca9.uscourts.gov/datastore/general/2013/12/27/11-17483_opinion122713.pdf.
11. S. Jacob, "Tuning in to Cellular Phone Calls Illegal, but Also Very, Very Popular," *Boston Globe*, 4 Feb. 1993.
12. D.G. Savage, "Court Lets Police Eavesdrop on Cordless Phones," *Los Angeles Times*, 9 Jan. 1990; http://articles.latimes.com/1990-01-09/news/mn-155_1_cordless-phone-transmissions.
13. "Preliminary Memorandum, January 5, 1990 Conference," no. 89-691, *Tyler, et al. v. Berodt, et al.*, 5 Jan. 1990; http://epstein.wustl.edu/research/blackmunMemos/1989/DM-1989-pdf/89-691.pdf.
14. S. Huang, "Recent Google Street View Court Decision Threatens to Criminalize Ordinary Wi-Fi Use (part 3): How the Court Reversed Itself, and How the Courts Should Analyze This Issue in the Future," *CSPRI Byte*, 23 Feb. 2014.
15. "*Joffe v. Google*, No. 11-17483, D.C. No. 5:10-md-02184-JW, Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of Appellees and Urging Affirmance," Apr. 2012; http://epic.org/amicus/google-street-view/EPIC-Streetview-Amicus-NDCal.pdf.
16. "*Joffe v. Google*, No. 11-17483, D.C. No. 5:10-md-02184-JW, Brief of Amicus Curiae Information Technology & Innovation Foundation in Support of Google's Petition for Rehearing and Rehearing En Banc," 4 Oct. 2013; www2.itif.org/2013-amicus-brief.pdf.
17. "18 U.S. Code § 1029—Fraud and Related Activity in Connection with Access Devices," Legal Information Inst., Cornell Univ.; www.law.cornell.edu/uscode/text/18/1029.
18. "In Re Innovatio IP Ventures, LLC Patent Litigation," MDL no. 2303, case no. 11 C 9308, US District Court, N.D. Illinois, Eastern Division, 22 Aug. 2012, pp. 889–895; http://scholar.google.com/scholar_case?case=16680089225036893693.
19. "AT&T Acceptable Use Policy," AT&T; www.corp.att.com/aup.
20. *18 U.S. Code § 1030—Fraud and Related Activity in Connection with Computers*, Legal Information Inst., Cornell Univ.; www.law.cornell.edu/uscode/text/18/1030.

Simson L. Garfinkel is an associate professor of computer science at the Naval Postgraduate School in Arlington, Virginia. His research interests include digital forensics, security, and privacy. Contact him at simsong@acm.org.

Michael McCarrin is a research associate in computer science at the Naval Postgraduate School in Monterey, California. His research interests include digital forensics and approximate matching algorithms. Contact him at mrmccarr@nps.edu.