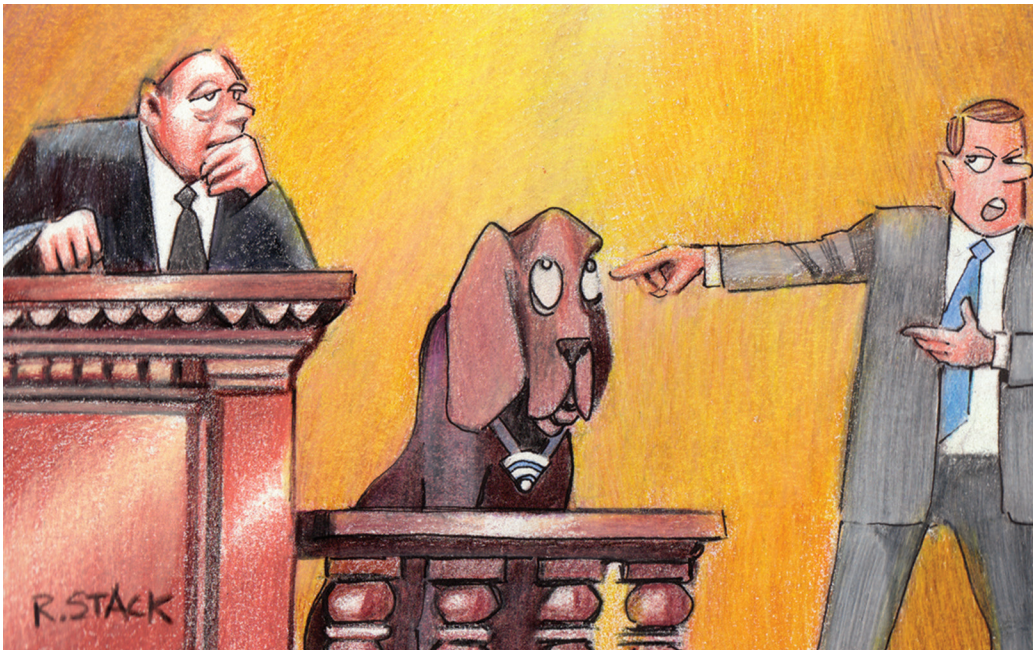
Editors: Alessandro Acquisti, acquisti@andrew.cmu.edu | Hugh Thompson, hthompson@peoplesecurity.com

Should Sniffing Wi-Fi Be Illegal?

Paul Ohm | University of Colorado Law School



On 21 December 1996, Mr. and Mrs. Martin of Fort White, Florida, were driving to the mall to do some Christmas shopping while listening to Mr. Martin's police scanner. Suddenly, they heard recognizable, famous voices—those of powerful Republican members of Congress, including then Speaker of the House Newt Gingrich. These politicians were crafting a response to ethics charges against Gingrich, which were going to be announced later that day. The Martins could hear the conversation because one person on the call, an up-and-coming congressman named John Boehner, was using an analog cell phone from his parked car, which they happened to be passing. The Martins recorded the call on a cassette and shared it with Representative Jim McDermott, then the Democratic ranking member of the House Ethics Committee, who leaked a transcript to several news outlets.

Soon, the Martins and McDermott learned firsthand several lessons about the unyielding seriousness of US wiretap laws, which said that they had illegally invaded the privacy of the people on that call. The Martins learned that the law treads not lightly on wiretapping, declaring it a felony punishable by up to five years in prison. Rather than risk this sentence, the Martins pled guilty to misdemeanors and paid fines of US$500 each. McDermott learned that the law prohibits not only the initial interception of private conversations but also the downstream use. Sued by Boehner, McDermott fought back, asserting a First Amendment defense. The court ultimately ruled against McDermott, finding that the admittedly important First Amendment values at stake were trumped by the vital purposes of wiretap laws and the need to deter other would-be wiretappers. The court ordered McDermott to pay more than $1 million dollars to cover Boehner's legal fees.

Flash forward several decades to another car, driving down another road, also surreptitiously scanning the airwaves, bearing even more sophisticated radio surveillance equipment. Google's famous Street View car intercepted and stored the headers and contents of data packets of anybody using Wi-Fi within range of its powerful antennas. (Although Google captured incomplete packets, still, according to one investigation, it ended up capturing email account passwords and the content of email messages.[1]) But what really separates Google's actions from the Martins' is scale. Google sniffed packets through not one but legions of Street View cars, over four years, in 30 countries. In total, the company collected 600 Gbytes of unencrypted, private information. We might never know for sure how many people had their private communications plucked out of the air by Google, but it seems plausible that they number in the millions.

Like the Martins and McDermott, Google has been embroiled in legal controversy ever since. US regulators have largely given Google a pass for its conduct, and as far as

we know, no criminal investigations were opened. But European regulators continue to press investigations into the alleged misconduct. In addition, a class-action lawsuit on behalf of those whose packets were intercepted, alleging a violation of the federal Wiretap Act, has thus far survived Google's motion to dismiss. Most recently, in September 2013, a federal appeals court rejected Google's motion, allowing the company's headaches to continue, if not compound.

I'll leave it for other times and people to untangle the difficult legal questions at this case's heart. (See, for example, Bruce Boyden's great series of blog posts.[2]) I ask instead, what should the law say about this? This fascinating question not only has ramifications for Wi-Fi and wiretapping but also poses broader questions about how we use law to protect online privacy. It leads us to consider many important and recurring debates on the collision of law and technology.

Maybe Sniffing Should Be Legal

Some people have argued that it should be legal to intercept communications transmitted over Wi-Fi. Their arguments take several forms. First, it shouldn't be illegal to do what's so easy to do. Criminalizing what's only "natural" seems to offend some deep sense of fairness. Second, and related, if people are so worried that others will learn what they transmit using Wi-Fi, they should encrypt their communications.

Third, even if wiretap laws protect privacy values, this benefit is outweighed by the benefits of unfettered access to the airwaves. Google claims that its Street View cars sniffed Wi-Fi packets to improve its map products. By compiling a database of the addresses of the world's Wi-Fi access points, Google can pinpoint your location on the globe (for your, or maybe advertisers', benefit) by recognizing the signatures of the access points in your proximity.

Finally, the potential criminalization of Wi-Fi sniffing seems to threaten crucial values of openness, experimentation, and curiosity. When Wi-Fi was still young, people memorably took to the streets toting Pringles cans[3] and modified laptops, searching, mapping, and sharing databases full of information obtained over open Wi-Fi networks. These *wardrivers* represented a link in a long chain of curious innovators, the kind of people who built the Internet. It would be an affront to declare what they do illegal.

On the Other Hand

As it happens, Congress has faced arguments like these before, and it's instructive to examine how it responded previously. In 1986, when Congress was contemplating extending wiretap laws to cover computer networks, some people argued that it shouldn't be illegal to intercept conversations conducted over cordless phones. These simple, analog devices broadcasted and received over only a few unencrypted channels, and they had the troublesome tendency to accidentally pick up nearby conversations.

Initially, Congress accepted these arguments, carving an exception to the law for cordless phones. Although this exception seemed to cover cordless phones but not cell phones, still, under it, the Martins and McDermott would have had one more argument for why their conduct hadn't been illegal.

But in the first few years of the law, Congress learned that the trouble this distinction caused outweighed the possible benefits. In 1992, it amended the law again, bringing cordless phones (and similar items such as baby monitors) into its prohibition. It helped that in the intervening years, technologists had introduced innovations such as channel hopping and scrambling to make accidental interception less likely.

Congress has acted once to tamp down arguments about the exceptionalist nature of radio communication; it should consider doing it again for Wi-Fi. This is because the arguments for the legality of sniffing might initially seem appealing but, on closer scrutiny, shouldn't carry the day.

The argument that things that are natural or easy to do shouldn't be illegal smacks of an unhelpful technological determinism. It treats technological developments as if they were products of nature, bestowed on us by some benevolent and mysterious force, one we should try not to subvert. This argument is misguided. Wi-Fi is simply a human product, one we should be able to control to avoid harm.

Also, what might be easy for experienced techies might not be easy for the average computer user, and our laws regulate the latter as much as the former (and there are many more of the latter, too). Even an average techie can find the software that modifies his or her operating system's networking stack to switch the interface into RFMON (Radio Frequency Monitor) mode, enabling his or her computer to capture packets. But how easily can the average network user do this? The vast majority of Wi-Fi users have never intercepted another user's packets and never will. Such behavior is rare and exceptional, even if it's easy for some. It seems much harder to believe that anybody can accidentally intercept Wi-Fi (much less the content of communications transmitted over it) in 2013 than it did to believe that people such as the Martins might accidentally intercept a cell phone call in 1996.

The argument that Wi-Fi sniffing's benefits can outweigh the harms to privacy is a red herring, at least in this case. Most wiretap laws apply only to collecting the contents

of communications, not merely to capturing addressing information transmitted in packet headers or Wi-Fi frames. If Google had restricted its collection to noncontent data such as SSIDs (service set identifiers) and MAC (media access control) addresses, as many Pringles-toting wardrivers have, it wouldn't have violated the Wiretap Act. (A separate law, the federal Pen Register and Trap and Trace Act, makes it a crime to use a device that collects "dialing, routing, addressing, and signaling information,"[4] but this law is far less punitive than the Wiretap Act. It's also almost never enforced.) Google has never sufficiently explained why it needed to capture packet content to aid its mapping efforts.

Although the benefits of sniffing packets and wardriving might be important, I believe they're outweighed by the privacy values on the other side of the balance sheet. At the very least, privacy is important because it protects us from harm. Any Google engineer with access to the 600-Gbyte database of sniffed packets might be able to read the email messages you sent and received and the webpages you visited, as well as pinpoint your location at that moment in time. If you ever had the misfortune to be using a computer in a cafe, office, or home along a Street View car's path, Google engineers can know all of this. Maybe you wouldn't consider this harmful because you have nothing to hide; your life is an open book. But it seems likely that at least some of the millions who were spied on would object vehemently to having that information known, even if only to Google's engineers.

The US Federal Bureau of Investigation (FBI) and the US National Security Agency (NSA) can also access Google's information—for example, to track the history of a fugitive or suspected terrorist (or, more troublingly, a political dissident or member of a religious minority). We don't know whether these agencies have accessed these data. However, given the recent revelations of NSA surveillance activities, it has become harder to argue that they lack the legal tools, desire, or sheer chutzpah to do such a thing.

Privacy has broader impacts too. Many have written about how we moderate our behavior when we think we're under a constant threat of surveillance. People tend to alter their thoughts and actions, avoiding the edgy or unorthodox, slowly sanding away the sharp corners of personality—and society. Citizens have difficulty expressing, reading, or shaping political opinions, destroying the prerequisites for a deliberative democracy. Pervasive surveillance can disempower, allowing the watchers to subtly control the watched.

People tend to alter their thoughts and actions, avoiding the edgy or unorthodox, slowly sanding away the sharp corners of personality—and society.

Protecting the Foundation of Privacy Law

To protect privacy's vital values, I propose a new way of thinking about privacy law: we have two types of privacy law, each doing very different types of work. On the one hand, we regulate the finer points of particular kinds of dataflows and data stores through laws tailored to particular industrial sectors. These laws include the Health Insurance Portability and Accountability Act (HIPAA) for health information, Family Educational Rights and Privacy Act (FERPA) for educational records, and Gramm-Leach-Bliley (GLB) Act for financial records. They're subtle and nuanced; you need a lawyer to understand them. In their ideal form, they strike a perfect balance, reflecting a carefully tailored risk assessment. We hope that a HIPAA-compliant hospital, FERPA-compliant school, or GLB-compliant bank will—merely by complying with the law—strike a reasonably good balance between mining the utility and safeguarding the privacy of data. But laws never achieve their ideal forms, meaning we doubt that today our laws strike this balance well. So, we tinker and hone, carving out exceptions here and bolstering protections there, to keep up with changing technological and societal conditions.

We need to build this layer of laws atop a firmer substrate made of bolder, broader laws. This second type of privacy law should help us construct meaningful boundaries between individuals and groups, and even between a single person's various personas, at least when these boundaries are desired. The lines these laws draw must be clear and easy for laypeople to understand. They needn't provide perfect privacy to all, but they should make very good privacy available to the motivated. These laws should never be riddled with exceptions and racked with subtlety. You should be able to understand them even if you haven't been to law school.

To me, the Wiretap Act has always been this second type of law. It was forged in the crucible of J. Edgar Hoover's aggressive surveillance tactics. Shortly after it was enacted, we were reminded of the need for it because of the Nixon administration's domestic surveillance that ultimately led to the Church Committee. Recent revelations about the NSA's seemingly boundless surveillance of the Internet drives home the need once again. The Act protects certain communication channels—telephones and

computer networks—from electronic surveillance, subject to a few narrow exceptions. It implements a fairly straightforward, unambiguous regime: don't intercept the content of communications without consent. If you do, don't disclose or use the information in any way, lest you commit a second crime. It's good that the courts have interpreted the Act broadly, overriding even objections raising important First Amendment values, as a reflection of the Act's important role.

But if we believe that the Wiretap Act plays a special, foundational role in protecting privacy, liberty, autonomy, and maybe even a flourishing, deliberative democracy, we must vigilantly protect it. We must reject calls to let it die a death of a thousand cuts. We should urge the opposite: Congress and the courts should reaffirm and strengthen its protections, and companies should avoid business models and legal arguments that eviscerate its safeguards.

This is why efforts to declare Wi-Fi sniffing legal under the Wiretap Act are so worrisome. According to the arguments made in Google's motion to dismiss, the law that declared the Martins potential felons and cost Representative McDermott $1 million dollars wouldn't apply to massive, invasive programs of data collection, simply because those data are sent using Wi-Fi. Under this interpretation, this bedrock privacy law would treat wired and wireless communication unequally and would drive a wedge between telephonic and computerized communication. Our bedrock of privacy protection would crumble with every technological advance. This isn't a tiny crack in the foundation of privacy law, it's a chasm that might undermine privacy law's entire structure.

Google needs to understand the ramifications of the arguments it has been making in litigation. It needs to consider that if its arguments prevailed—and, mercifully, they haven't yet—any interception of Wi-Fi would no longer be prohibited, whether done by well-meaning companies, nefarious identity thieves, or the government. Google has argued that its interceptions were innocent and unknown, at least to managers. But its arguments would empower others with far more pernicious goals to conduct massive surveillance with impunity. I bet that FBI lawyers are silently cheering Google on from the sidelines. If Google's arguments ever carry the day, the FBI could sit outside cafes hoovering up the communications of everybody inside, with no suspicion, without violating the statute. (To be sure, it still might be violating its own internal rules or the US Constitution.)

Congress could easily save us from this possibility. As it did back in 1992 when cordless phone calls' privacy wasn't assured, Congress should amend the Wiretap Act to unambiguously reaffirm that intercepting the contents of communications sent over Wi-Fi is a crime. So much is at stake. ■

References

1. P. Sayer, "Google's Street View Wi-Fi Data Included Passwords, Email," *Infoworld*, 18 June 2010; www.infoworld.com/d/networking/googles-street-view-wi-fi-data-included-passwords-email-679.
2. B. Boyden, "Why Google's Wi-Spy Argument Is Stronger Than It First Appears," blog, 19 Aug. 2013; http://madisonian.net/2013/08/19/why-googles-wi-spy-argument-is-stronger-than-it-first-appears.
3. R. Block, "WiFi Cantennas Now 'Illegal'," 25 July 2005; www.engadget.com/2005/07/25/wifi-cantennas-now-illegal.
4. US Code, Title 18, sections 3121 and following.

Paul Ohm is an associate professor at the University of Colorado Law School. Contact him at paul.ohm@colorado.edu.