2017

Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis

Riana Pfefferkorn

Follow this and additional works at: https://opencommons.uconn.edu/law_review

Recommended Citation

https://opencommons.uconn.edu/law_review/373
Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?

RIANA PFEFFERKORN

Encryption shields private information from malicious eavesdroppers. After years of slow adoption, encryption is finally becoming widespread in consumer-oriented electronic devices and communications services. Consumer-oriented encryption software is now more user-friendly, and much of it turns on encryption by default. These advances enhance privacy and security for millions of people.

However, encryption also poses an impediment to law enforcement’s ability to gather electronic evidence. Law enforcement calls this the “going dark” problem. U.S. law enforcement agencies have responded through both legal and technological means to encryption’s perceived threat to their capabilities. The scope of encryption’s impact on those capabilities is not yet clear, and police still have a wealth of data and technical tools at their disposal. Nevertheless, sophisticated criminals can use encryption to stymie investigators, forcing them to resort to resource-intensive, tailored measures to investigate those individuals.

One means of doing so is through a “side-channel attack.” Our electronic devices are always radiating something—electromagnetic emissions, heat, and so forth. Those emissions reveal information, called “side channel information,” about the device. The physical implementation of a cryptosystem leaks electromagnetic emissions from which academic researchers have shown it is possible to extract the system’s secret encryption keys. Side-channel cryptanalysis is not a known law enforcement tactic at present, but that may change in time.

Law enforcement use of side-channel attacks will raise Fourth Amendment issues that will require a fact-intensive analysis to resolve. In determining what legal process (if any) will authorize a side-channel attack, a court will have to carefully examine what information will be acquired, from where, and how. The Supreme Court’s Fourth Amendment jurisprudence does not provide clear, predictable guidance for those inquiries. Its decision in Kyllo v. United States supplies the touchstone for the legal analysis of side-channel attacks. However, the Court’s current framework for electronic surveillance cannot adequately safeguard Americans’ privacy interests from erosion by technological advances.
Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?

RIANA PFEEFFERKORN

INTRODUCTION

“Everything vibrates.”1 Actually, “everything radiate[s].”2 Every physical implementation of a cryptosystem leaks something—electromagnetic radiation, power consumption, sound, or some other emission. Those leakages can be measured, and those measurements reveal information—likely against the cryptosystem user’s wishes and without her knowledge.

In cryptography, these sources of indirect information are called side channels. A side-channel attack on a cryptosystem seeks to gain information from physical leakages, rather than by other, more direct methods of cryptanalysis.

At present, side-channel attacks are (to our knowledge) the business of America’s military and intelligence agencies, not its police. They are typically complex and resource-intensive, limiting their feasibility for law enforcement use. That said, such attacks have become more affordable over time, and technologies that originated in military and intelligence use have a tendency to trickle down to garden-variety police departments. Meanwhile, as commercially-available, relatively easy-to-use encryption software gains widespread favor among Americans, law enforcement officials have been exploring options for circumventing encryption to gain access to data and communications in intelligible form. In time, law enforcement may seek to resort to certain types of side-channel attack to gather information after exhausting other means of investigating a sophisticated, high-value target.


When that time comes, investigators will have to consider whether the Fourth Amendment regulates their gathering of side-channel information. Do the police need a warrant to obtain information about a target through a side-channel attack? That’s the question this Article seeks to answer. The conclusion: It depends.

I. WHAT IS SIDE-CHANNEL CRYPTANALYSIS?

Cryptography is the discipline of protecting secrets through coded writing. Encryption is “the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge...” An encryption algorithm turns human-readable language (“plaintext”) into an unintelligible scramble (“ciphertext”) that ostensibly can only be decoded using a decryption key. Encryption keeps the encoded information secret from anyone who is not intended to have access to it, even if that person has access to the ciphertext.

Cryptanalysis is “the flip-side of cryptography:” the study of code-breaking. There are a number of different methods of modern cryptanalysis. One class of techniques exploits weaknesses in the encryption algorithm. For example, an algorithm may produce seemingly random ciphertext that in fact contains patterns which the attacker...
(“cryptanalyst”) can analyze to crack the secret code.\footnote{For example, an attacker can apply “frequency analysis” to ciphertext, checking which letters occur most often; she guesses that they correspond to the most frequent letters in English (assuming the plaintext is in English), and guesses the rest of the letters from there. Simon Singh, \textit{Letter Frequencies}, Simon Singh, \url{http://www.simonsingh.net/The_Black_Chamber/letterfrequencies.html} (last visited Feb. 6, 2017).}

Another class of techniques, called \textit{side-channel attacks}, gains information about the targeted cryptosystem\footnote{A cryptosystem “is a general term referring to a set of cryptographic primitive[] tools] used to provide information security services. Most often the term is used in conjunction with primitives providing confidentiality, i.e., encryption.” \textit{HAC}, supra note 4, at 15. Put more simply, “[a] cryptosystem is pair of algorithms that take a key and . . . convert plaintext to ciphertext and back.” Bellovin, \textit{Intro}, supra note 7, at 4.} by exploiting weaknesses in its physical implementation.\footnote{See \textit{François Koeune et al., A Tutorial on Physical Security and Side-Channel Attacks, in Foundations of Security Analysis and Design III 78–108 (2005) [hereinafter Koeune].}} Side-channel cryptanalysis works by measuring information that the physical implementation of the cryptosystem emits through \textit{side channels}.\footnote{See, e.g., \textit{Liang Cai & Hao Chen, TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion 1 (2011) [hereinafter TouchLogger], \url{https://www.usenix.org/legacy/event/hotsec11/tech/final_files/Cai.pdf} (describing how it is possible to log keystrokes on smartphones with touchscreens, due to the fact that “keystroke vibration[s] on touch screens are highly correlated to the keys being typed”) (paper delivered at 6th Usenix Workshop on Hot Topics in Security (HotSec’11)); see also Zhi Xu \textit{et al., TapLogger: Inferring User Inputs On Smartphone Touchscreens Using On-Board Motion Sensors 2 (2012), \url{http://www.cse.psu.edu/~sxz16/papers/taplogger.pdf} (indicating that keystrokes can be inferred through motion sensor data) (paper delivered at the Fifth ACM Conference on Wireless Network Security (WiSec 2012)). Both of these publications assume that the smartphone’s user installs malware that reads the data from the phone’s motion sensors and transmits it back to the attacker, i.e., that the side-channel information is being measured directly from the device, not remotely. Similarly, recent research demonstrated an in-browser JavaScript-based side channel attack (i.e., no app download needed) that can infer user PINs with high accuracy using side-channel information from a mobile device’s motion and orientation sensors. \textit{Maryam Mehrnezhad et al., Stealing Pins Via Mobile Sensors: Actual Risk Versus User Perception} (2016), \url{https://arxiv.org/pdf/1605.05549v1.pdf} [hereinafter Stealing Pins].} Side-channel information includes motion,\footnote{See, e.g., Adi Shamir \& Eran Tromer, \textit{Acoustic Cryptanalysis: On Noisy People and Noisy Machines, https://www.cs.tau.ac.il/~tromer/acoustic/ec04rump} [May 4, 2004] (materials presented at the Eurocrypt 2004 rump session in Interlaken, Switzerland) (describing how a CPU in the midst of particular computations may create auditory signatures that could be used to decrypt secret keys).} sound emitted during a computation,\footnote{See, e.g., \textit{Adi Shamir \& Eran Tromer, Acoustic Cryptanalysis: On Noisy People and Noisy Machines, https://www.cs.tau.ac.il/~tromer/acoustic/ec04rump} [May 4, 2004] (materials presented at the Eurocrypt 2004 rump session in Interlaken, Switzerland) (describing how a CPU in the midst of particular computations may create auditory signatures that could be used to decrypt secret keys).
electromagnetic (EM) emissions,\textsuperscript{17} cryptographic hardware’s power consumption,\textsuperscript{18} and the time it takes a computer to execute a cryptographic algorithm,\textsuperscript{19} to name a few examples.

One goal of cryptanalysis is for the cryptanalyst to determine the cryptosystem’s secret key.\textsuperscript{20} The keys to encrypt devices and communications differ. The keys to encrypt a device reside on the device and do not leave it.\textsuperscript{21} For the encryption of communications, the keys to encrypt a particular communication (“session keys”) are exchanged between the two parties, but each party’s long-term identity key (which lets the parties prove their identities to each other) stays on the device.\textsuperscript{22}

A side-channel attack that allows the attacker to obtain the cryptosystem’s secret encryption key is called a key-recovery attack\textsuperscript{23} or

\begin{footnotesize}
\begin{itemize}
\item See, e.g., KOEUNE, supra note 13. In 1985, Wim van Eck was the first to publish an unclassified technical paper on EM side-channel attacks, specifically focusing on attacks against computer monitors. See Wim van Eck, Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?, 4 COMPUT. & SEC. 269, 270 (1985) (discussing how it is “possible to reconstruct the picture displayed on [a] video display unit from the radiated emission”). EM side-channel attacks are therefore also called “van Eck phreaking,” though the term properly refers only to EM side-channel attacks to reproduce the display of a monitor. CRAIG BAUER, SECRET HISTORY: THE STORY OF CRYPTOLOGY 344 (2013).
\item See, e.g., Paul Kocher et al., Differential Power Analysis, 1999 INT’L ADVANCES IN CRYPTOLOGY CONF. 2 (discussing SPA, a technique for collecting information about a device’s cryptographic operations by directly interpreting power consumption measurements).
\end{itemize}
\end{footnotesize}
key-extraction attack. This Article focuses on electromagnetic side-channel key-recovery attacks. In recent years, researchers “have demonstrated that they can recover the keys from the major types of public key encryption in use today simply by picking up the radio waves emanating from your laptop.” The Article examines whether law enforcement can take advantage of that capability without legal process.

The latest public research on side-channel cryptanalysis has its roots in World War II and the early Cold War era. During the war, the military bought encryption devices that turned out to leak EM emissions that allowed the recovery of plaintext from eighty feet away. In the 1950s, the newly-created National Security Agency (NSA) tested its equipment and realized that all of it radiated EM emissions. The agency took defensive countermeasures and set specifications for shielding equipment from spying. These so-called TEMPEST attacks are low-cost to conduct, but expensive to defend against, as they are “non-trivial . . . and can require a lot of special equipment.” Military standards for equipment shielding are largely classified, which limits the academic and private sectors’

---


25 While this Article focuses on key-recovery attacks, the author hopes it provides a framework for thinking through Fourth Amendment issues with respect to other varieties of side-channel attack as well.


28 Johnson, supra note 2, at 221.

29 See BAUER, supra note 17, at 343 (“[V]arious countermeasures were taken to minimize the distance at which emanations could be measured to reveal information.”). The countermeasures are called TEMPEST (Transient Electromagnetic Pulse Emanation Standard), and while the term technically refers only to defensive measures, side-channel attacks that exploit EM emanations are commonly called “TEMPEST attacks.” Id.

30 van Eck, supra note 17, at 270. The attack van Eck described, against a cathode-ray tube (CRT) monitor, required only a TV set and about $15 in additional equipment. Id. A more recent attack against a liquid-crystal display (LCD) monitor allegedly cost less than $2,000 in equipment. See BAUER, supra note 17, at 344 (citing Markus G. Kuhn, ELECTROMAGNETIC EAVESDROPPING RISKS OF FLAT-PANEL DISPLAYS 23–25 (2004) [hereinafter Electromagnetic Eavesdropping Risks of Flat-Panel Displays] 23–25 (2004) [hereinafter Electromagnetic Eavesdropping Risks], https://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf [https://perma.cc/F7ZF-J387] (paper presented at 4th Workshop on Privacy Enhancing Technologies in Toronto, Can.).

31 BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 220 (2000).
opportunities to come up with low-cost countermeasures.32

Part of what makes TEMPEST attacks so costly to defend against is that the issue affects all kinds of electronic equipment. Since “everything radiate[s]” electromagnetic emissions,33 EM side-channel attacks are not limited to monitors. “[E]verything leaks to some degree,” be it cell phones, fax machines, computer switches, cables, power lines,34 or keyboards.35

EM side-channel attacks, while powerful, are currently of limited utility “in the field.” A major concern for anyone conducting a side-channel attack is being discovered by the target. The attacker must not be detected—or at least, the target must not realize the attack is happening. Because they involve measuring physical outputs such as EM emissions or sound, side-channel attacks typically require placing the attacker’s sensing equipment in close physical proximity to the system being attacked.36

EM attacks on monitors can work at enough of a distance to quell a would-be attacker’s fears: hundreds of meters for old CRT monitors,37 and ten38 to thirty meters39 for newer flat-screen displays.

32 MARKUS G. KUHN, COMPROMISING EMANATIONS: EAVESDROPPING RISKS OF COMPUTER DISPLAYS 85–86 (2003), https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf [https://perma.cc/HJ7C-74A3] (“Secret ‘Tempest’ specification will not enjoy the continued quality assurance offered by public scrutiny and open academic research. Such peer review and feedback has led in the past repeatedly to significant improvements of technical standards, for example, in cryptology, even where open research initially lags a decade or two behind the classified state of the art.”).

33 Johnson, supra note 2, at 221.

34 SCHNEIER, supra note 31, at 220.

35 See Martin Vuagnoux & Sylvain Pasini, Compromising Electromagnetic Emanations of Wired and Wireless Keyboards 1 (2009), https://www.usenix.org/legacy/events/sec09/tech/full_papers/vuagnoux.pdf [https://perma.cc/3HH3-3KRJ] (“Explaining that EM side-channel attacks on wired and wireless keyboards allowed researchers to recover up to 95% of the keystrokes entered, meaning that most modern computer keyboards “are not safe to transmit confidential information,” such as passwords) (paper presented at 18th Conference on USENIX Security Symposium in Montreal, Can.).

36 See KUHN, supra note 32, at 133 (“Eavesdropping on unintended hardware emissions usually requires a physical presence close to the target. This can lead to significant cost and risk of discovery for the eavesdropper.”). Of course, proximity is unnecessary if the target transmits side-channel data directly to the attacker—such as where the attacker can get the target to download and run malicious code on an electronic device that “phones home” to the attacker with the data. See supra note 15 and accompanying text. The legal requirements for law enforcement to do this are beyond the scope of this Article. See infra notes 129, 133 and accompanying text.

37 van Eck, supra note 17, at 270–71 (stating that it is not possible to decrease the radiation from the electron beam in the CRT).

38 See ELECTROMAGNETIC EAVESDROPPING RISKS, supra note 30, at 8 fig.3 (illustrating that text is readable from ten meters away); see also Tom Simonite, Seeing Through Walls, NEW SCIENTIST (Apr. 20, 2007, 6:59 PM), https://www.newscientist.com/blog/technology/2007/04/seeing-through-walls.html [https://perma.cc/75VC-EKEY] (stating that Professor Kuhn reported successfully seeing flat-panel displays from up to twenty-five meters away and claimed that he “was able to eavesdrop [on] certain laptops through three walls”).

Side-channel key-extraction attacks in particular, however, typically require far greater proximity. One recent EM key-extraction attack cleverly fits the sensing equipment inside a piece of pita bread, but the attack is effective only at distances of twenty centimeters to half a meter.40 The same researchers also demonstrated an acoustic key-extraction attack against laptops that works at a distance of four meters, so long as the attacker uses a parabolic microphone; the attack can also be accomplished using just a mobile phone, but with an effective distance of only thirty centimeters.41 Likewise, the same team’s recently-published electromagnetic key-extraction attack against an Apple iPhone required “placing a magnetic probe in the proximity of the device.”42

The same (eerily prolific) team recently demonstrated an EM key-extraction attack against laptops that works by measuring, through a wall, the EM leakage of a target laptop located in an adjacent room.43 The attack still requires proximity,44 but the wall provides coverage for the attacker (and any conspicuous equipment) from discovery by the target.

TEMPEST-style attacks on displays may be more practical than other varieties of electromagnetic side-channel attack,45 but key-recovery attacks have their advantages. A TEMPEST attack, though feasible at greater
distances, only lets the attacker “see” whatever the target happens to display on his monitor. Obtaining the target’s secret encryption keys unlocks the door to a much greater cache of information.

In sum, side-channel key-recovery attacks can be a powerful way to circumvent a target’s use of encryption and gain access to his records in plaintext. However, they will remain limited in investigatory utility until they can work at greater distances and with discreet equipment. The next Section discusses why law enforcement may nevertheless need to deploy such attacks in the future, regardless of their drawbacks.

II. ENCRYPTION AND ITS DISCONTENTS

A. Encryption Is Growing in Popular Use (at Last)

Encryption started out being too important to let just anybody use it. But in the digital age, it has become too important for anybody not to use it. We rely on encryption to secure our communications, medical records, banking records, financial transactions, business secrets, intellectual property, and national security. Nowadays, just about everybody gets to have encryption, and consumer-oriented encryption software is finally making some progress in overcoming its longstanding usability problems.

Secret writing goes back centuries, yet despite its long and distinguished history in warfare, intelligence, and statecraft, 46

46 See ELECTROMAGNETIC EAVESDROPPING RISKS, supra note 30, at 8 fig.3 (stating that text is readable from ten meters away through three walls).
50 Julius Caesar used a cipher to protect his confidential writings. See SUETONIUS, THE CAESARS 100 (Donna W. Hurley trans., 2011) (“And whenever he writes in code, he substitutes B for A, C for B,
cryptography has only come into widespread use by laypeople relatively recently. For many years, the NSA jealously guarded all information about crypto and hindered its dissemination in the civilian sphere. That changed with the rise of the Internet in the late twentieth century, following a pitched battle in the courts and Congress. The history of the so-called “Crypto Wars” of the 1990s has been amply documented already and need not be revisited here. Suffice it to say that as of this writing, in the United States, it is legal as a general matter to teach cryptography and to sell encryption software and cryptographic equipment (albeit with some restrictions on exports).

It took a while for average Americans to show much enthusiasm for this hard-won outcome. But they cannot be faulted for that. Encryption has contributed for years to the ongoing tension between security and usability. Commercial, off-the-shelf encryption software has long been notoriously user-unfriendly, difficult to configure properly, and clunky to

and the rest of the letters that follow in the same plan.

Also, the Founding Fathers encoded their letters discussing an early draft of the First Amendment. See John A. Fraser, III, The Use of Encrypted, Coded and Secret Communications Is an “Ancient Liberty” Protected by the United States Constitution, 2 VA. J.L. & TECH. 1, 43 (1997) (describing how correspondence between Jefferson and Madison concerning comments to the First Amendment consisted of partially enciphered text).

Steven Levy, Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age 13–15 (2001) (describing how “all the salient information about modern crypto was withheld from public view” by the shadowy NSA, which “considered itself the sole repository of cryptographic information in the country—not just that used by the civilian government and all the armed forces, . . . but that used by the private sector as well”).

Id. This source is an excellent, readable account of the Crypto Wars that is accessible to those without a mathematical or scientific background (such as the author, and the non-negligible segment of the legal community that decided to go to law school because there is no math on the LSAT).

See Junger v. Daley, 209 F.3d 481, 483, 485 (6th Cir. 2000) (challenging then-current export restrictions on encryption software, likewise holding encryption software source code to be First Amendment-protected speech, in case brought by a professor who wished to disseminate encryption software source code as part of a course on computers and the law); see also Bernstein v. U.S. Dep’t of Justice, 176 F.3d 1132 (9th Cir. 1999) (ruling, in narrow holding, that software source code is speech protected by the First Amendment, and that government regulations unconstitutionally prevented publication of cryptographic source code which plaintiff Daniel Bernstein wanted to publish while a student at the University of California, Berkeley), reh’g en banc granted and opinion withdrawn, 192 F.3d 1308 (9th Cir. 1999).


See, e.g., Scott Ruoti et al., Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client (2016), https://arxiv.org/pdf/1510.08555v2.pdf [https://perma.cc/4KF5-C4CY] (reporting results of a usability study of the encrypted email client Mailvelope, with the majority of study participants finding it difficult to use and almost none of the participants being able to successfully complete the tasks assigned to them, thus leading to the conclusion that “[u]sable, secure email is still an open problem more than 15 years after it was first studied”).

“For encryption to help most citizens, it has to be usable. It often is not.” Calo, supra note 6, at 37. See, e.g., Alma Whitten & J.D. Tygar, Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0, in Security and Usability: Designing Secure Systems That People Can Use 679, 699
use. 59 Unsurprisingly, because “encryption was typically cumbersome” in the past, “its use [was] rare.” 60

In recent years, developers have finally started to make “usable security” a visible priority. Companies such as Apple, Facebook, and Google have implemented strong encryption into their products and services, in some instances turning encryption features on by default. 61 “Defaulting to encryption” is preferable to making users configure their settings, because “something that is already turned on need not be usable, and most people stick with defaults, making encryption widespread.” 62

For communications security, Apple uses default “end-to-end” encryption in its iMessage messaging app and FaceTime video call app, 63 meaning the two interlocutors can read the messages they exchange, but eavesdroppers cannot read any intercepted plaintext—and neither can Apple. 64 Open Whisper Systems’ free Signal app for text messages and voice calls is also end-to-end encrypted by default. 65 Facebook-owned WhatsApp now uses Signal’s encryption protocol to encrypt messages, voice calls, and video calls end-to-end by default. 66 End-to-end encryption for email remains a thorny challenge, however—Google and Yahoo

(Lorrie Faith Cranor & Simson Garfinkel eds., 2005) (reporting the dismal results of a usability assessment of version 5 of Pretty Good Privacy [PGP], a tool for encrypting email).

59 Whitten & Tygar, supra note 58, at 680.
61 See Alan Z. Rozenshtein, Surveillance Intermediaries, 70 STAN. L. REV. (forthcoming 2018), at *32 (citations to draft dated Mar. 17, 2017, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2935321 [https://perma.cc/E8WB-RQWH]). Rozenshtein claims that “regular Internet users don’t use PGP and Tor because both systems are difficult to use.” Id. (citing Whitten & Tygar, supra note 58; further citations omitted). He lays this problem at the feet of “open-source developers [who] lack the resources and organization to make them sufficiently user-friendly for widespread use,” whereas large companies like Apple and WhatsApp “have the money and talent,” as well as “legal and social clout,” “to build end-to-end encryption into their services so seamlessly that users communicate securely without even realizing it.” Id.
62 Calo, supra note 6, at 39; see also Rozenshtein, supra note 61, at *33 (“the vast majority of users never bother to change those (or any other) default settings”) (citation omitted).
64 Id. (“Apple has no way to decrypt iMessage and FaceTime data when it’s in transit between devices. So unlike other companies’ messaging services, Apple doesn’t scan your communications, and we wouldn’t be able to comply with a wiretap order even if we wanted to.”).
65 OPEN WHISPER SYSTEMS, https://whispersystems.org/ [https://perma.cc/S3W5-6J5X] (last visited Feb. 7, 2016) (“We cannot read your messages, and no one else can either. Everything is always end-to-end encrypted and painstakingly engineered in order to keep your communication safe.”).
encrypt email messages in transit between user and server, but have yet to roll out end-to-end encryption despite years of effort.

The trend of improved encryption offerings extends to the encryption of data at rest as well. Apple encrypts iPhones and iPads by default; in fact, it does not allow users to disable device decryption. Mobile phones running Google’s Android mobile operating system can also be encrypted, although Android device encryption rates have lagged far behind iPhone’s for several reasons. Those challenges have hampered Google’s efforts to turn on default device encryption.

Beyond smartphones, there are also options for encrypting data stored on computers and in the cloud. Disk encryption is available for Apple, Microsoft, and Linux operating systems, though Apple and Microsoft do not turn this feature on by default. Finally, while they face their own set

---


71 Kaveh Waddell, Encryption Is a Luxury, ATLANTIC (Mar. 28, 2016), https://www.theatlantic.com/technology/archive/2016/03/the-digital-security-divide/475590/ [https://perma.cc/Q5N8-DQU5]. The gap between iPhone and Android perpetrates a “digital divide” along race and class lines: users of expensive iPhones tend to be well-educated and high earners, whereas less-costly Android phones, which have a majority market share, are primarily used by low-income people and African-Americans—the very segments of the population most heavily surveilled by the government. Id.


of challenges when it comes to encryption.\textsuperscript{74} Cloud storage providers such as Dropbox and Box encrypt users’ files at rest in the cloud.\textsuperscript{75}

Encryption tools are still far from perfect when it comes to usability\textsuperscript{76} and “defaulting to encryption.” And tradeoffs that favor either greater security or greater usability are an unavoidable part of life.\textsuperscript{77} Nevertheless, the welcome trend in crypto implementation by major U.S. companies with massive user bases means that hundreds of millions of people in the U.S. and worldwide finally have some fairly usable ways to protect their communications and stored data.

B. “Going Dark” and Novel Forms of Electronic Evidence-Gathering

The rise in communications and device encryption is a boon for user security. Law enforcement, however, has responded with dismay. Encryption makes information-gathering more difficult for law enforcement, and the more prevalent it becomes, the more that challenge grows. It is not clear that the problem is as serious as the authorities claim, particularly given the many sources of information still available to them. Nevertheless, law enforcement has been exploring other options, both legal and technological, for maintaining their surveillance capabilities as encryption grows ever more ubiquitous.

1. “Going Dark”? Or . . .

Encryption does not just keep hackers and criminals from accessing someone’s data; it can stymie law enforcement, too. Even if investigators obtain proper legal process to intercept communications in transit or to access data at rest, encryption poses a technological barrier to carrying out


\textsuperscript{76} See, e.g., Jonathan Geater, Why Johnny STILL Can’t Encrypt (Feb. 17, 2017) (presentation given at RSA Conference in San Francisco, Cal.) (abstract and recording of presentation available at https://www.raconference.com/events/us17/agenda/sessions/6352-why-johnny-still-cant-encrypt [https://perma.cc/TT22-ZZ8N]) (arguing that the application program interfaces (APIs) for encryption tools are what need to be fixed, not users).

\textsuperscript{77} Renowned computer security expert Bruce Schneier has criticized the “‘either/or’ thinking” of “security and usability as a trade-off,” wherein “a more secure system is less functional and more annoying, and a more capable, flexible, and powerful system is less secure.” This mindset, he says, perversely leads to “systems that are neither usable nor secure.” Bruce Schneier, Security Design: Stop Trying to Fix the User, SCHNEIER ON SECURITY (Oct. 3, 2016, 6:12 AM), https://www.schneier.com/blog/archives/2016/10/security_design.html [https://perma.cc/E38K-KN4J].
the order. Law enforcement calls this issue “going dark”: criminals and terrorists will use encryption to cloak their activities from police eyes.

Law enforcement officials have been sounding warnings about encryption for over twenty years. When the issue first arose in the 1990s, the “going dark” battle in the Crypto Wars culminated in a compromise. Since 1994, the federal Communications Assistance for Law Enforcement Act (CALEA) has required telecommunications carriers to make their systems wiretappable for law enforcement so that Americans’ phone calls do not “go dark.” However, carriers may provide encryption and need not maintain decryption capabilities.

“Information services” (understood originally to mean Internet-related businesses and companies that set up operations online) are not included in the access mandate, meaning “[t]he Internet was completely exempted” from CALEA’s coverage.

These exceptions were less consequential in practical effect when CALEA was first enacted than they are today. As noted, encryption software was persistently user-unfriendly for a long time, so it understandably did not come into widespread use in the early years following CALEA’s passage. Between the guaranteed wiretappability of phone calls and the limited public adoption of encryption software, law enforcement’s “going dark” nightmare future failed to materialize.

In recent years, however, CALEA’s “information services” exemption has taken on greater significance. “Information services” include email providers, messaging apps, social media services, and computer and smartphone manufacturers. Providers of those services have taken advantage of their legal freedom to offer encrypted consumer-oriented products and services. Now, with advances in user-friendliness and either ready availability or default implementation in many popular devices and

79 Id.
80 Steven Levy, Battle of the Clipper Chip, N.Y. TIMES (June 12, 1994), http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all [https://perma.cc/JW9Y-X4SS] (“Law-enforcement and intelligence agencies contend that if strong [cryptographic] codes are widely available, their efforts to protect the public would be paralyzed... If cryptography is not controlled, wiretapping could be rendered obsolete.”).
83 Id. § 1002(b)(3); see also Albert Gidari, CALEA Limits the All Writs Act and Protects the Security of Apple’s Phones, CTR. FOR INTERNET & SOC’Y (Feb. 19, 2016, 6:26 PM), https://cyberlaw.stanford.edu/blog/2016/02/calea-limits-all-writs-act-and-protects-security-applephones [https://perma.cc/3HJ7-RUKL].
84 47 U.S.C. § 1002(b)(2); Geller, supra note 81.
85 See Geller, supra note 81 (defining “information services” and showcasing how many modern features of internet communication are exempt).
services, encryption protects millions of people’s communications, devices, and stored records. The upshot is that law enforcement can no longer expect reliable, easy access to the plaintext contents of electronic communications and stored data of people they investigate or prosecute.

As encryption has finally become widespread, law enforcement officials have revived their anti-encryption arguments from the 1990s. The FBI renewed its warnings to the public in 2008 (when the phrase “going dark” appears to have been coined), and continued beating the drum in testimony to legislators over the next few years, even drafting legislation that would have closed the CALEA “information services” exemption.

Proponents of the “going dark” viewpoint found new cause for alarm in late 2014. Apple and Google announced that they were reworking the encryption in their respective mobile operating systems, such that they would no longer have the capability they had previously maintained to extract data from passcode-locked devices for police—even with a warrant. The law enforcement community swiftly condemned these changes. The FBI’s director said the two companies were “allow[ing] people to place themselves beyond the law.”

---

86 See supra Section II.A.
87 See Going Dark, supra note 78 (discussing how the growing encryption of web traffic makes it harder for police to eavesdrop on a target’s online activities); see also Finley, supra note 67 (discussing how the rise of HTTPS has hampered law enforcement’s ability to eavesdrop on Internet traffic).
91 See Timberg, supra note 90 (referencing comments by the former head of the FBI’s criminal investigative division on how default encryption is “problematic”).
attorney published a heated op-ed in the Washington Post, claiming that the changes gave free rein to criminals and calling for congressional action if Apple and Google did not reverse them.\footnote{Cyrus R. Vance Jr., Apple and Google Threaten Public Safety with Default Smartphone Encryption, WASH. POST (Sept. 26, 2014), https://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43a9bf0-44ab-11e4-b437-1a7368204804_story.html [https://perma.cc/3N7P-N8VG].} To date, however, encryption continues to make gains, with no sign of retreat.\footnote{See, e.g., Finley, supra note 67 (noting that at least half of all web traffic is encrypted); Metz, supra note 66 (discussing the ongoing implementation of end-to-end encryption into WhatsApp).}

2. *A “Golden Age of Surveillance”?*


One point critics note is law enforcement’s reliance on anecdotes and incomplete data. Officials cite individual instances of deplorable crimes for which investigators could not unlock smartphones that might contain evidence,\footnote{See, e.g., MANHATTAN DIST. ATTORNEY’S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY’S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 9 (2015) [hereinafter DA 2015 REPORT], http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Encryption%20and%20Public%20Safety.pdf [https://perma.cc/7XNA-2W5Z] (stating that prosecutors were unable to access smartphones in cases involving “homicide, attempted murder, sexual abuse of a child, sex trafficking, assault, and robbery”); Peter Holley, A Locked iPhone May Be the Only Thing Standing Between Police and This Woman’s Killer, WASH. POST (Feb. 26, 2016), https://www.washingtonpost.com/news/post-nation/wp/2016/02/26/a-locked-iphone-may-be-the-only-thing-standing-between-police-and-this-womans-killer/ [https://perma.cc/JT9Z-XPD6] (prosecutors sought to access the locked iPhone of a murdered pregnant woman).} without contextualizing the rarity of the “worst of the worst” crimes compared to run-of-the-mill offenses.\footnote{See Riana Pfefferkorn, James Comey’s Default-Encryption Bogeyman, JUST SECURITY (Jan. 15, 2016, 12:15 PM), https://www.justsecurity.org/28852/comeys-default-encryption-bogeyman/ [https://perma.cc/D682-AN8Z] (discussing how law enforcement’s public statements regarding “going dark” focus on how encryption helps criminals engaged in murders and sex crimes, when in reality the typical cases in which law enforcement is likely to encounter encryption are probably low-level drug offenses).} Likewise, reporting in isolation the number of smartphones prosecutors have in custody but
cannot unlock leaves a crucial question: do prosecutors obtain convictions in those cases anyway? It appears they often do. If law enforcement can still successfully prosecute cases despite encryption, then the “going dark” issue is not (yet) as consequential as claimed.

The fact that an individual’s devices or communications are encrypted does not leave police empty-handed. Even with the growing ubiquity of encryption, numerous sources of metadata, and even content information, are still available to investigators through the usual channels of legal process. Professor Peter Swire coined the phrase “golden age of surveillance” to describe the sea of data law enforcement can now access, such as where people have been, who they know, and “databases that create digital dossiers about individuals’ lives.” These “massive gains,” he argues, have “more than offset” the losses attributable to encryption.

There is some evidence to support his contention. Encryption appears not to have significantly hindered wiretaps yet. Also, law enforcement

---


99 See Pfefferkorn, supra note 97 (stating that the DA 2015 REPORT does not mention “whether prosecutors successfully pursued those cases using other evidence; the total number of search warrants issued for smartphones during the period cited; how many of those devices turned out to be encrypted; and of those, how many warrants were successfully executed nevertheless.”).


101 Encryption’s impact on law enforcement will shift over time, but it is too early to tell how. Encryption Workarounds, supra note 60, at 41.

102 See Peter Swire, The Golden Age of Surveillance, SLATE (July 15, 2015, 4:12 PM), http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html [https://perma.cc/MEP2-LF6G] (discussing how the use of metadata and location information is available to law enforcement agencies, and that encryption need not be weakened to give those agencies tools to fight crime).

103 Id.

104 Id.

105 See Steven M. Bellovin et al., Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, 12 NW. J. TECH. & INTELL. PROP. 1, 14–15 & 14–15 nn.59–60 (2014) (analyzing federal wiretap reporting data showing very few wiretaps where investigators encountered encryption and concluding that law enforcement will rarely have to resort to unusual methods in order to carry out
can still access the plaintext contents of most text messages sent, despite
the growing popularity of encrypted messaging apps. The prevalence of
Android phones may account for this. Over half of U.S. smartphones are
Android phones, whose default messaging option is not encrypted end-
to-end. Most people do not change defaults, so a significant
percentage of Android users’ (and, given Android’s market share, the
general public’s) text messages will still be accessible by law enforcement.
The same goes for device encryption, since most Android devices are not
encrypted by default. In short, Android’s market dominance and defaults
likely mitigate encryption’s impact on law enforcement.

Even where the plaintext contents of messages cannot be intercepted—and
we know of a few cases where WhatsApp and iMessage encryption supposedly stymied wiretap orders—metadata about the messages typically remains available from the provider (with Signal a notable exception). Metadata is highly useful in law enforcement

Title III wiretaps); see also Lorenzo Franceschi-Bicchierai, Feds and Cops Encountered Encryption in Only 13 Wiretaps in 2015, VICE: MOTHERBOARD (June 30, 2016 1:30 PM), https://motherboard.vice.com/en_us/article/wiretap-report-feds-and-cops-encountered-encryption-in-only-13-wiretaps-in-2015 [https://perma.cc/9Z3S-KMJN] (“Once again, for the second straight year, the number of times [that] state or federal wiretaps [ ] encountered encryption, decreased . . . .”). But see Bellovin et al., supra, at 105 (“Even if law enforcement does not currently have a serious problem in conducting authorized wiretaps, with time it will.”).

106 Swire, supra note 102.
107 Waddell, supra note 71.
108 Id.
109 Calo, supra note 6, at 39.
110 Cunningham, supra note 70.
111 What is more, the groups most likely to be targeted for surveillance are the very people who tend to use Android phones, Waddell, supra note 71—meaning the choice of whom to surveil helps predict the (un)likelihood of encountering encryption when doing so.

112 See Matt Apuzzo, WhatsApp Encryption Said to Stymie Wiretap Order, N.Y. TIMES (Mar. 12, 2016), https://www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html?_r=0 (“No decision has been made, but a court fight with WhatsApp, the world’s largest mobile messaging service, would open a new front in the Obama administration’s dispute with Silicon Valley over encryption, security and privacy.”).

113 See Matt Apuzzo, David E. Sanger, & Michael S. Schmidt, Apple and Other Tech Companies Tangle with U.S. Over Data Access, N.Y. TIMES (Sept. 7, 2015), https://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html (reporting “several” cases in which Apple “rebuffed” iMessage wiretap requests). The Department of Justice (DOJ) reportedly shelved the idea of taking Apple to court over its inability to comply. Id.

114 Swire, supra note 102. Apple and WhatsApp retain messaging metadata, which they produce to law enforcement pursuant to valid legal process; Apple has even disclosed the phone numbers to which an iMessage user started composing an ultimately unsent message. Sam Biddle, Apple Logs Your iMessage Contacts—And May Share Them with Police, THE INTERCEPT (Sept. 28, 2016, 10:00 AM), https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police/. Signal, by contrast, retains minimal metadata; in response to a subpoena, it can disclose only the time an account was created and the account’s date of last connection to Signal’s servers. Cyrus Farivar, FBI Demands Signal User Data, But There’s Not Much to Hand Over, ARS TECHNICA
investigations because it “leaves traces of every electronic communication a suspect has, showing whom they speak to, how often, how long, and from where,” allowing investigators to reconstruct a detailed picture of an individual’s activities and contacts (and their activities and contacts). Access to metadata is not a 100% replacement for access to content, but it remains a powerful tool for law enforcement investigations.

For content information, police can turn to remote storage sources in lieu of intercepts or seizures of data from encrypted devices. Professor Swire argued several years ago that encryption was prompting a shift in law enforcement strategy from real-time intercepts of data, which were becoming more likely to be encrypted in transit, to seeking stored data, especially in the cloud. Cloud storage services’ encryption practices do not necessarily preclude them from compliance with government requests for content information. WhatsApp lets users back up their messages, but stores them in a form that is readable by WhatsApp (and thus by law enforcement). The same is true of Signal backups. Apple encrypts user data stored in iCloud, but it can, and does, disclose iCloud-stored user


116 See Encryption Workarounds, supra note 60, at 28–29 (discussing options available within the “locate a plaintext copy” category of encryption workarounds and setting forth the necessary requirements for the search to succeed).


119 See Shelton, supra note 66 (noting that WhatsApp allows users to back up their media and messages to the cloud, but the data is not protected by WhatsApp’s end-to-end encryption while in Google Drive or while in iCloud).


information (which can include numerous categories of data) to law enforcement. Android users can back up their data to Google Drive (if their phone model supports it), where the backups are accessible to law enforcement with a warrant. In short, the rise of cloud storage has mitigated the effects on law enforcement investigations of the concurrent rise of device and messaging encryption.

Other sources of information with considerable potential for law enforcement use are the Internet of Things (IoT) and existing vulnerabilities in consumer software and hardware. The new technologies that make our lives more convenient can also make us easier to surveil—for example, by turning the on-board driver assistance system in our cars into a roving wiretap, or monitoring our homes through an IoT-connected device. The burgeoning IoT opens up a whole new world

---

123 See Brian Barrett, How Apple Could Make Your iPhone and Mac Even More Secure, WIRED (June 10, 2016, 6:59 PM), https://www.wired.com/2016/06/apple-security-improvements/ [https://perma.cc/BFTY-GASX] (noting that Apple often “hands” over data to law enforcement when asked) and can do so because “while iCloud backups are encrypted, Apple maintains a copy of the keys”); Andy Greenberg, Two Tips to Keep Your Phone’s Encrypted Messages Encrypted, WIRED (Apr. 26, 2016, 9:00 AM), https://www.wired.com/2016/04/tips-for-encrypted-messages/ [https://perma.cc/GL3X-BBQE] (noting that messages backed up to Apple’s iCloud servers are “open to all the usual risks of exposure to hackers, to Apple . . . or to any government that can force those companies to turn over the data”); APPLE, REPORT ON GOVERNMENT INFORMATION REQUESTS: JANUARY 1–JUNE 30, 2016 (2016), https://www.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf [https://perma.cc/5YCX-KJW9] (stating that the company will “provide customers’ iCloud content, which may include stored photos, email, iOS device backups, documents, contacts, calendars, and bookmarks” in response to a search warrant).

124 See Jason Cipriani, What You Need to Know about Encryption on Your Phone, CNET (Mar. 10, 2016, 5:00 AM), https://www.cnet.com/news/iphone-android-encryption-fbi/ [https://perma.cc/65HL-J29J] (“As with Apple’s iCloud Backup practices, data within a backup stored on Google’s servers is accessible by the company when presented with a warrant by law enforcement”).

125 The Internet of Things (“IoT”) is a “network of internet-connected objects able to collect and exchange data using embedded sensors.” It specifically “refers to the connection of devices (other than typical fare such as computers and smartphones) to the Internet, including “[c]ars, kitchen appliances, and even heart monitors.” See Andrew Meola, What is the Internet of Things (IoT)?, BUS. INSIDER (Dec. 19, 2016, 2:11 PM), http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8 [https://perma.cc/AMT8-UTCL] (explaining the Internet of Things and providing a glossary of terms and basic definitions).

126 This idea dates back at least fifteen years, to when the FBI sought to use a vehicle’s on-board driver-assistance system “as a roving ‘bug.’” Company v. United States, 349 F.3d 1132, 1133–34 (9th Cir. 2003). The Ninth Circuit rejected the government’s argument that a provision of the Wiretap Act required the service provider to comply with court orders compelling the provider’s assistance, because “FBI surveillance completely disabled the monitored car’s [s]ystem,” in violation of the Wiretap Act’s requirement that any technical assistance must be “accomplish[ed] . . . with a minimum of interference” to the service provided. Id. at 1145–47; 18 U.S.C. § 2518(4) (2012) (describing the requirements for an “order authorizing or approving the interception of any wire, oral, or electronic communication” and indicating that such an order must be accomplished “unobtrusively and with a minimum of interference”).

of audio, video, and metadata that can be repurposed from consumer to law enforcement use, “as long as [such uses] are appropriately authorized, resourced, and overseen.”

Surveillance through the IoT will repurpose intentional features of IoT devices. Law enforcement also exploits bugs—unintentional flaws—in commercial software products. The government has been exploiting software vulnerabilities to catch suspected criminals for most of this century. Recently, the government evidently exploited a browser vulnerability to hack over a thousand computers on the basis of a single warrant. “[G]overnment hacking can raise complex legal questions under the Fourth Amendment and other laws,” and unsurprisingly, the legality of that single warrant has been challenged in numerous prosecutions that stemmed from the operation. But while exploiting

panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/5L7E-28XU] [hereinafter DON'T PANIC] (detailing how “[t]he audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications”).

See Matt Apuzzo, F.B.I. Used Hacking Software Decade Before iPhone Fight, N.Y. TIMES (Apr. 13, 2016), https://www.nytimes.com/2016/04/14/technology/fbi-tried-to-defeat-encryption-10-years-ago-files-show.html?r=0 [https://perma.cc/P77U-CR2Z] (describing how the FBI was using spyware as part of a criminal wiretap as early as 2003); Kevin Poulsen, Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years, WIRED (Apr. 16, 2009, 9:33 PM), https://www.wired.com/2009/04/fbi-spyware-pro/ [https://perma.cc/GTL2-7U5R] (describing how the FBI has been using spyware to infiltrate computers for at least seven years as part of its criminal investigations). Hacking by the government is a complex topic that was well addressed—from technical and policy standpoints, not a legal one—in Lawful Hacking. See generally Bellovin et al., supra note 105 (providing a comprehensive discussion of hacking by the government).

See Joseph Cox, The FBI’s ‘Unprecedented’ Hacking Campaign Targeted over a Thousand Computers, MOTHERBOARD (Jan. 5, 2016, 4:00 PM), https://motherboard.vice.com/en_us/article/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers [https://perma.cc/N7Z5-46SY] (detailing the FBI’s hack over a thousand computers to fight “what it has called one of the largest child pornography sites on the dark web”).

Encryption Workarounds, supra note 60, at 26.

existing security vulnerabilities in computer systems may be a legally chancy strategy.\textsuperscript{133} That means investigators will have plenty of low-hanging fruit to pluck when they seek to circumvent encryption and gain access to a target’s computer, without any need to resort to a side-channel attack.\textsuperscript{135}

In the view of “going dark” critics, encryption is far from leaving law enforcement in the dark. Whether that will continue to be true remains to be seen, and will depend in part on the success of various “encryption workarounds,” both legal and technological.\textsuperscript{136}

3. Law Enforcement’s Legal and Technological Responses to “Going Dark”

Notwithstanding the numerous sources of information available to them and the unclear extent of the “going dark” problem, law enforcement officials have nevertheless advocated for both legal and technological measures to counteract what they call “warrant-proof” encryption’s\textsuperscript{137} effects on their information-gathering capabilities. As this subsection will explain, law enforcement has asked legislatures to change the law and courts to authorize novel strategies for gathering digital evidence.

\textsuperscript{133} Law enforcement has long been aware of the suppression risks associated with its hacking activities. One early strategy “became so popular with federal law enforcement that Justice Department lawyers in Washington warned that overuse of the novel technique could result in its electronic evidence being thrown out of court in some cases.” Poulsen, supra note 129. A March 7, 2002 memo from the Department of Justice warned that use of the spyware program raised “difficult legal questions” and suppression risks “without any countervailing benefit.” See id. (internal quotation marks omitted).

\textsuperscript{134} Bellovin et al., supra note 105 at 27–28 (explaining that vulnerabilities will never go away despite programmers’ best efforts to engineer all the bugs out of their code).

\textsuperscript{135} KUHN, supra note 32, at 133 (observing in 2003 that EM side-channel attacks were not yet a “practically relevant information security threat,” and that “[t]he vast majority of practical vulnerabilities can be exploited using comparatively simple and purely software-based techniques”; adding caustically, “[t]his is likely to remain the case, as long as information security is only a secondary consideration in the design and selection of products, equally neglected by both product designers and end users.”).

\textsuperscript{136} See Encryption Workarounds, supra note 60, at 4, 40. Kerr and Schneier set forth six categories of encryption workarounds: “find the key,” “guess the key,” “compel the key,” “exploit a flaw,” “access plaintext when in use,” and “locate a plaintext copy.” Id. at 9–29. Electromagnetic key-recovery attacks are not discussed in the article, but come closest to a combination of “find the key” and “exploit a flaw.”

Simultaneously, law enforcement agents rely on digital forensics tools and “hacks” to circumvent the encryption they encounter during investigations.

The past two years have seen legislative proposals at both the state and federal level concerning law enforcement’s access to encrypted information. At state level, bills introduced (unsuccessfully) in three states, including one based largely on the Manhattan district attorney’s model bill, would have either forced or induced smartphone manufacturers to ensure that law enforcement could access encrypted smartphones.

In the Senate, two senators drafted a bill last year to require covered entities (such as smartphone makers) to comply with court orders for information by either providing it in “intelligible” form or supplying any technical assistance “necessary” to render encrypted data intelligible. The bill would have effectively closed the “information services” exemption in CALEA, though it did not acknowledge this impact. After digital security experts roundly condemned the bill, its authors quietly let it die on the vine. Subsequently, despite earlier testimony that he would not seek “going dark” legislation, then-FBI Director Comey vowed to raise the issue anew this year to the new Congress and administration.

---


139 A.B. 1681, 2016 Reg. Sess. (Cal. 2016) (bill that would have penalized makers of smartphones and mobile operating systems which they cannot decrypt for law enforcement); H.B. 1040, 2016 Reg. Sess. (La. 2016) (bill that would have also penalized makers of smartphones and mobile operating systems which they cannot decrypt for law enforcement); A.B. A8093, 2016 Leg. Sess. (N.Y. 2015) (bill to require smartphones to be decryptable for law enforcement).


141 Id.


143 See David Kravets, Obama Administration Won’t Seek Encryption-Backdoor Legislation, ARS TECHNICA (Oct. 9, 2015, 4:00 PM), https://arstechnica.com/tech-policy/2015/10/obama-administration-wont-seek-encryption-backdoor-legislation/ [https://perma.cc/TA6H-GHEQ] (“Comey said the administration for now will continue lobbying private industry to create backdoors to allow the authorities to open up locked devices to investigate criminal cases and terrorism.”).

In the courts, law enforcement has tried several legal strategies for gaining access to encrypted information. Federal and state law enforcement agents have sought to compel people to provide passcodes or fingerprints to unlock their encrypted smartphones, raising Fifth Amendment issues. The law in this area is still evolving, and the analysis is highly fact-dependent. With regard to passphrases, courts have come out in different ways depending on the particulars of the case. When it comes to fingerprints, the government has had more uniform success. In the few known instances to date that involve the issue, courts have typically let compelled fingerprint-unlocking go forward.

See Encryption Workarounds, supra note 60, at 19 (“How the ‘foregone conclusion’ doctrine applies to compelled decryption is presently uncertain. The open question is what facts must be established as known by the government to make the testimony implicit in decryption a foregone conclusion.”); see generally id. at 15–21 (discussing the “practical and legal hurdles rather than technical ones” that arise in the “compel the key” category of encryption workaround).

Compare Florida v. Stahl, 206 So. 3d 124, 132, 136–37, (Fla. Dist. Ct. App. 2016) (reviewing cases “that have addressed the Fifth Amendment implications for providing decryption keys and passcodes[], which have largely applied the act-of-production doctrine and the ‘foregone conclusion exception’” and concluding that the act of providing the phone’s passcode was not testimonial and that the foregone conclusion exception applied), with In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1346–49 (11th Cir. 2012) (collecting the cases that had addressed the passcode issue at that time and concluding that the Fifth Amendment protected the defendant’s refusal to decrypt his encrypted devices “because the act of decryption and production would be testimonial, and because the Government cannot show that the ‘foregone conclusion’ doctrine applies”), and United States v. Apple Mac Pro Computer, 851 F.3d 238, 248 n.7 (3d Cir. 2017) (questioning in dicta whether the correct focus of the foregone conclusion analysis is on “the Government’s knowledge of the content of the [encrypted] devices” or instead “on whether the Government already knows the testimony that is implicit in the act of production”). See generally Sarah Wilson, Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand Over Passwords, 30 BERKELEY TECH. L.J. 1, 14–27 (2015) (hereinafter Wilson, Compelling Passwords) (surveying and discussing Fifth Amendment passcode cases).


E.g., State v. Diamond, 890 N.W.2d 143, 149–51 (Minn. Ct. App. 2017), review granted, No. A15-2075 (Minn. Mar. 28, 2017) (holding such compulsion not a Fifth Amendment violation); In re Search Warrant Application for [Redacted], No. 17-M-85, 2017 U.S. Dist. LEXIS 169384 (N.D. Ill. Sept. 18, 2017) (not a Fifth Amendment violation if police, with a warrant, apply fingers of home’s four residents onto iPhone’s TouchID sensor); In re Search of iPhone Seized from 3254 Altura Ave. in Glendale, Cal., No. 2:16-mj-00398, slip op. at 4 (C.D. Cal. Mar. 15, 2016), https://ia601603.us.archive.org/2/items/gov.uscourts.cacd.641321/gov.uscourts.cacd.641321.3.0.pdf [https://perma.cc/8FHY-S79V] (search warrant authorizing law enforcement agents to depress individual’s fingerprints onto seized iPhone’s TouchID sensor); To Beat Crypto, supra note 147 (discussing two other fingerprint-unlocking search warrants); see also Wilson, Compelling Passwords, supra note 146, at 28 n.164 (citing cases that have allowed compelled fingerprint unlocking to go forward).
The government has argued for aggressive interpretations of federal law in support of its alleged surveillance and investigative authority. The FBI relied on the Stored Communications Act (SCA) and the Pen Register Act’s technical-assistance provision to obtain court orders and a seizure warrant compelling encrypted email service provider Lavabit to hand over its private Secure Socket Layer (SSL) encryption keys. A federal appeals court declined for procedural reasons to decide whether those statutes in fact permit the seizure of encryption keys.

The DOJ has also obtained dozens of orders compelling Apple and Google to bypass the passcodes of locked, encrypted iPhones and Android phones for which law enforcement had a warrant, in order to extract data from the phones. It advocates for an expansive interpretation of the federal All Writs Act (AWA) that would allow courts to enlist private non-parties such as Apple into assisting in investigations. While the

---


151 Id. § 3124(a) (2012) (“Upon the request of [a government agent], a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish [the agent] forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference . . . .”).


154 For a map of all known cases, see All Writs Act Orders for Assistance from Tech Companies, ACLU, https://www.aclu.org/map/all-writs-act-orders-assistance-tech-companies [https://perma.cc/86WQ-2M7J] (last visited Feb. 9, 2017).

155 The AWA permits federal courts to “issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a).

AWA does allow courts to issue orders to non-parties, it is not clear how far it can be stretched.\(^\text{157}\) Only two courts have issued public opinions analyzing these orders' propriety, and they came out opposite ways.\(^\text{158}\)

Again on the basis of the AWA, the government asked for an unheard-of form of novel technical assistance when it wanted access to a passcode-locked iPhone running iOS 9 which had been used by one of the perpetrators of the December 2015 terror attack in San Bernardino, California.\(^\text{159}\) The government sought, and originally received, an AWA order compelling Apple to write a custom version of iOS for installation on the phone.\(^\text{160}\) Rather than targeting the iPhone’s encryption, the custom software instead would roll back other security features that prevented law enforcement from running a program to “brute-force” guess the phone’s passcode.\(^\text{161}\) After a short but feverish legal battle popularly dubbed “Apple vs. FBI,” the government dropped the case when it gained access to the phone by purchasing an exploit from an undisclosed vendor.\(^\text{162}\) The court vacated its original order to Apple\(^\text{163}\) without addressing the merits of the

\(^{157}\) See United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977) (observing that the AWA allowed a court to issue an order binding a non-party because there was no other way for the government to carry out its court-authorized surveillance, the non-party was not too “far removed from the underlying controversy,” and compliance with the order would not be unduly burdensome).

\(^{158}\) Compare In re Order Requiring XXX, Inc., No. 14 MAG. 2258, 2014 U.S. Dist. LEXIS 154743, at *3–4 (S.D.N.Y. Oct. 31, 2014) (concluding that under the AWA, “it is appropriate to order the manufacturer here to attempt to unlock the cellphone so that the warrant may be executed as originally contemplated”), with In re Apple, Inc., 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016) (concluding that the AWA does not permit the relief the government sought, and even if it did, the government’s application did not satisfy the factors a court may use in deciding whether to issue a requested writ).


\(^{160}\) Nakashima, supra note 159.


\(^{163}\) Apple v FBI Timeline, supra note 162.
FBI’s broad legal arguments, leaving the AWA’s scope still undefined.164

“Apple vs. FBI” shows that law enforcement need not rely on pushing aggressive legal theories in order to get help in circumventing encryption. Law enforcement has a long history of exploiting hardware and software vulnerabilities to “hack” into suspects’ electronic devices.165 Federal, state, and local police also use digital forensics tools to crack passcodes and extract data from devices.166 Such tools are now commonplace in city police departments nationwide.167 Police can get data off locked devices, recover deleted text messages and photos, and access data in the cloud, all without assistance from service providers or smartphone makers.168

Between government hacking and third-party digital forensics devices, police have a number of technological tools available to get access to electronic evidence. These technological means further call into question law enforcement’s claim that encryption’s rise is causing it to “go dark.”

C. Side-Channel Attacks Aren’t a Feasible Law Enforcement Technique—Yet

The availability of so many options for information-gathering makes it seem somewhat premature to discuss the constitutionality of warrantless side-channel attacks. The police probably are not using side-channel attacks at present and probably won’t for a while yet. Investigators won’t resort to difficult, high-tech surveillance strategies unless the amount of plaintext and metadata available through established surveillance

164 Alina Selyukh, Apple vs. the FBI: The Unanswered Questions and Unsettled Issues, NAT'L PUBLIC RADIO (Mar. 29, 2016, 3:20 PM), http://www.npr.org/sections/alltechconsidered/2016/03/29/472141323/apple-vs-the-fbi-the-unanswered-questions-and-unsettled-issues [https://perma.cc/Q3E8-6XY3]; see also Encryption Workarounds, supra note 60, at 30 (predicting that “the degree of third-party assistance that can be legally compelled is likely to be a continuing theme of the law of encryption workarounds”).

165 See Bellovin, supra note 105, at 31–32, 43 (addressing the government’s exploitation of vulnerabilities, the warrant issues that arise in this context, and the vulnerability and exploit markets); see supra Section II.B.2 and notes 137–38.


168 Joseph, supra note 167.
mechanisms, government hacking, and forensics tools really does plummet.

Side-channel attacks are not only unnecessary at present, they are impractical. Agents need to buy the requisite equipment, learn to use it correctly, and position it (and usually themselves) close to the target’s device(s) for as long as needed to accomplish the attack. The equipment needed is usually conspicuous and/or very limited in range. What is more, even after collecting the side-channel information, agents have to take additional steps to convert the raw data they collected into information they can actually use: the target’s secret encryption key. This means having specialist personnel on hand (i.e., a trained computer scientist), and the process may fail multiple times before a key is extracted successfully.169

These considerations make side-channel attacks much less attractive than traditional police methods, established electronic-surveillance methods, and digital forensics. Tailing a target in person takes up agents’ time, but it does not take a Ph.D. in computer science to learn how to do it. Fully-remote surveillance (such as carrying out a Title III wiretap) is more convenient than having to monitor a target from nearby. Getting the target’s emails from his service provider may cost money, but paying out a reimbursement to the carrier170 (which maintains all the servers, stores all the data, and does all the work) is more straightforward than equipment procurement, assembly, testing, and training. Digital forensics devices cost money, too, but the costs are relatively modest171—and, notably, many

---

169 For example, in one recently-demonstrated electromagnetic key-extraction attack on mobile devices, after measuring an iPhone’s electromagnetic emanations, actually extracting the secret encryption key required multiple steps of signal processing and cryptanalysis; the final step alone took two hours, and the researchers successfully recovered the secret key only twice out of thirty tries. See ECDSA Key Extraction, supra note 42, at 13–14.

170 See 18 U.S.C. § 2706 (2012) (requiring the government to pay a fee to service providers when it “obtain[s] the contents of communications, records, or other information” from them under certain sections of the Stored Communications Act, as “reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information”); cf. 18 U.S.C. § 2518(4) (2012) (requiring compensation for wiretap assistance); 18 U.S.C. § 3124(c) (2012) (requiring compensation for assistance with pen registers and trap-and-trace devices).

cities’ police departments already have them.172

In short: side-channel attacks cost money, time, personnel, expertise, and convenience. Law enforcement has yet to “go dark” enough for such burdensome undertakings to start looking like a viable option.173 But that day is coming. The FBI predicted in 2011 that as encryption becomes ubiquitous, most criminals will stay unsophisticated enough to keep getting caught, but the agency will occasionally need to craft burdensome “individualized solutions” for “very sophisticated target[s]” who encrypt their communications (such that not even the third-party carriers can decrypt them for law enforcement).174

At the same time, the development of side-channel attacks keeps pace with the current generation of consumer electronics in popular use: from CRT monitors175 to flat-screen displays,176 from typewriters177 to iPhones and iPads.178 And the attacks keep coming down in price and complexity of the equipment involved.179 If law enforcement believes its need to resort to “individualized solutions” will increase over time, while the cost and complexity of side-channel attacks will continue to decrease, then eventually, those two trend lines will intersect. That is the point where

172 Joseph, supra note 167; Waltman, id.
173 See Swire, supra note 102.
174 Pell, supra note 89, at 622 (quoting 2011 congressional testimony of then-FBI general counsel Valerie Caproni on the “going dark” issue). “In other words, time, energy, and resources must be expended to determine how to acquire data about a specific target that would otherwise be readily available from third parties with an appropriate court order without all these additional transaction costs.” Id. at 625.
175 See van Eck, supra note 17.
176 Electromagnetic Eavesdropping Risks, supra note 30, at 1, 2 (discussing the popular use of flat-screen display devices by consumers).
177 In the early 1980s, Soviet spies conducted acoustic side-channel attacks against IBM Selectric typewriters in the U.S. Embassy in Moscow: they bugged the typewriters with tiny microphones that allowed them to hear each key struck and thereby determine each individual letter being typed. SHARON A. MANEKI, CTR. FOR CRYPTOLOGIC HIST., NAT’L SEC. AGENCY, LEARNING FROM THE ENEMY: THE GUNMAN PROJECT 1, 14–21 (2012), https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/assets/files/gunman-project/Learning_From_the_Enemy_The_GUNMAN_Project.pdf [https://perma.cc/F7BB-ACJF].
178 See ECDSA Key Extraction, supra note 42, at 2.
179 In 2012, a key-extraction attack conducted by analyzing mobile devices’ radio-frequency (RF) emissions cost $1,000 in equipment. GARY KENWORTHY & PANKAJ ROHATGI, MOBILE DEVICE SECURITY: THE CASE FOR SIDE CHANNEL RESISTANCE 1 (2012), https://pdfs.semanticscholar.org/4d1c/e909dfe6d9476cd5a1f546a98388468a4d.pdf [http://perma.cc/7LPQ-DL76]. In 2016, Genkin et al. demonstrated a “cheap low-bandwidth key extraction attack[]” against mobile devices that cost a little over $50 in scavenged or eBay-bought equipment, distinguishing it from previous attacks that had “used expensive lab-grade equipment, such as oscilloscopes, for their measurements.” ECDSA Key Extraction, supra note 42, at 1, 16, 18. Similarly, the same Genkin team had demonstrated a key-extraction attack against various laptop computers in 2015 that “us[ed] simple and readily available equipment, . . . [or] alternatively, . . . a common, consumer-grade radio,” both of which “avoid the expensive equipment used in prior attacks, such as low-noise amplifiers, high-speed digitizers, sensitive ultrasound microphones, and professional electromagnetic probes.” STEALING KEYS FROM PCS, supra note 40, at 4, 5.
side-channel attacks will make the jump from military and intelligence use to law enforcement use.

When side-channel attacks eventually do become a law enforcement technique, the first to use them will be federal law enforcement, which, as noted, already anticipates the need for tailored solutions for individual targets. ¹⁸⁰ Last year, the FBI asked Congress for over $38 million just to develop and acquire tools to counter encryption’s impact on the FBI’s information-gathering abilities. ¹⁸¹ It is not clear from the request just what tools the FBI contemplates, but equipment for side-channel cryptanalysis can be interpreted to fall within the category of “cryptanalytic capability” tools listed in the request. ¹⁸²

At the state and local level, where budgets are more constrained, police probably won’t deploy side-channel attacks against suspects unless and until they become less labor- and resource-intensive. That said, the FBI partners with state and local law enforcement agencies around the country to conduct digital evidence examinations and give digital forensics trainings. ¹⁸³ Those partnerships could extend in future to the FBI’s loaning its side-channel attack expertise to state and local police. ¹⁸⁴

What is more, state and local law enforcement agencies have a well-established track record of eventually obtaining technologies that originated for military or intelligence use. Defense contractor Harris Corporation’s “Stingray” surveillance device, a “cell-site simulator” that allows police to extract data from cell phones by mimicking a wireless carrier’s cell tower and forcing the phone to connect to it, was originally

¹⁸⁰ See Pell, supra note 89, at 622 (quoting Caproni testimony discussing law enforcement’s development of methods to overcome encryption used by criminal targets).


¹⁸² See FBI 2017 BUDGET REQUEST, supra note 181, at 2-1.


¹⁸⁴ See Encryption Workarounds, supra note 60, at 30, 33–35 (differing resource levels could “lead to the federal government taking over certain kinds of state and local investigations,” depending on the workaround needed; not every workaround “require[s] technical expertise and deep pockets” like federal law enforcement authorities have).
developed for the military and intelligence community. Thanks in part to grants by the Department of Homeland Security (DHS), Stingrays and other cell-site simulators are now in widespread use by police departments around the country—which have gone to great lengths to keep the details secret from the courts, local governments, and the public. So, too, “mobile X-ray vans” first used in Afghanistan are now in (highly secretive, inadequately overseen) use by New York City police “to look through the walls of buildings or the sides of trucks.”

It thus takes no great stretch of the imagination to envision a near future where first the FBI and then garden-variety police departments begin adopting the intelligence community’s side-channel techniques for circumventing encryption, if the price is right. The equipment for conducting side-channel attacks could become the latest device handed down to local law enforcement authorities, with the FBI supplying the expertise to carry off the attack and DHS (read: taxpayers) footing the bill.

D. Hypothetical: Investigating a Sophisticated Crypto-Using Criminal

What would a near-future side-channel cryptanalysis operation look like? Side-channel attacks are likely to be deployed by law enforcement—if at all—only in very particular circumstances. Picture a high-value criminal target who uses encryption to shield his communications and stored data from prying eyes. He also uses a password manager to log into his accounts. The police have obtained wiretap orders to intercept the

---


186 Id.

187 Joseph, supra note 167 (enumerating city police departments nationwide that have purchased cell phone surveillance tools). Joseph’s article describes the unusually powerful “Dirtbox” cell-site simulator, which was used by the NSA for mass surveillance in France and which Baltimore police have owned since 2012. Id.


190 A password manager obviates the need to manually enter one’s password when logging into one’s accounts. Lucian Constantin, 5 Things You Need to Know about Password Managers, PCWORLD (June 18, 2016, 6:34 AM) [hereinafter 5 Things], http://www.pcworld.com/article/3085395/security/5-things-you-should-know-about-password-managers.html [https://perma.cc/5374-3A55]. A password manager can frustrate an attacker’s attempt to learn a target’s account passwords via side-channel
target’s communications (such as phone calls, email, and text messages) and warrants to search and seize his stored data (such as documents in cloud-storage accounts, or emails stored on his email provider’s servers). However, they have been able to obtain only minimal, incomplete, or irrelevant information from the service providers the suspect uses. Intercepting his phone calls, email, and text messages in transit proves fruitless, as they are encrypted end-to-end and the police are unsuccessful in obtaining plaintext.191 He has turned off backups wherever possible, uses a messaging app that does not store copies of messages on its servers,192 and has encrypted the documents and email he stores on his service providers’ servers using a separate, extra layer of encryption beyond that built into the service.193 This renders the service providers unable to decrypt the stored files for law enforcement.194

information from his computer display (since the letters are not showing up in cleartext on the screen as he types them in), keyboard, or smartphone touchscreen (since he is not tapping in his account passwords). See TouchLogger, supra note 15 (discussing smartphone touchscreen side-channel attacks); TapLogger, supra note 15 (same); Stealing Pins, supra note 15 (discussing revealing PINs using data from smartphone’s motion and orientation sensors); Vuagnoux & Pasini, supra note 35 (discussing side-channel attacks on keyboards). True, the attacker could learn the master password the target uses to log into his password manager. That would be a serious security breach, as the master password is a “single point of failure” that would compromise all of the accounts managed by the password manager. See 5 Things, supra. But learning the master password is less valuable to a side-channel attacker if the password manager is the “offline” kind, i.e., it does not sync across devices and the master password is never sent to the password management service provider. Id. Even if the attacker gleans the master password through a side-channel attack, he won’t be able to log into the target’s password manager (and from thence into all the target’s accounts) unless he gains direct physical access to the device—in which case the game is already over.

191 They do succeed sometimes in real investigations, according to the Wiretap Reports transmitted annually to Congress by the United States Courts. The reports include information on the number of wiretaps where investigators “encountered” encryption (to wit: very, very few) and whether they were nevertheless able to obtain plaintext (to wit: sometimes). The reports do not reveal how investigators were able to get plaintext in the instances where they succeeded, or what (if any) methods they tried that failed. See Wiretap Reports, U.S. COURTS, http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports [https://perma.cc/83CE-TANS] (last visited Sept. 8, 2017) (repository of annual reports going back to 1997).


193 This “belt and suspenders” option adds an extra layer of protection to data in the cloud. As discussed, cloud service providers typically can provide user data to law enforcement in plaintext form pursuant to a warrant, even if the provider encrypts the stored information. See supra Section I.B.3 & note 142. Several programs allow users to encrypt their files before uploading them to cloud storage. E.g., Cale Hunt, How to Encrypt Data Before Storing It in the Cloud (and Why You Should), WINDOWS CENT. (Mar. 28, 2017, 7:00 AM), http://www.windowscentral.com/how-encrypt-data-storing-it-cloud-and-why-you-should [https://perma.cc/4EE8-EGXB].

194 As noted supra in Section II.B.1, “information services” such as cloud storage providers are not required by federal law to build law enforcement surveillance capabilities into their systems. 47 U.S.C. § 1002(b)(2) (2012). And even entities that are so mandated are not responsible for decrypting data unless they provided the encryption and have the ability to decrypt the data. Id. § 1002(b)(3).
In short, the usual avenues of gathering electronic evidence are closed off. But without the target’s unencrypted data and communications, law enforcement does not have enough information for a conviction, maybe not even enough to show probable cause for an arrest. To keep pursuing this investigation, they will need to craft a more individualized approach.

One rather blunt option with encryption-savvy suspects is to get the necessary warrants, then grab the target’s laptop or phone off him in public while he is using it.\(^\text{195}\) If he has his device and accounts open, then he already entered his passphrases to unlock them, and the police can access his unencrypted data.\(^\text{196}\) But that may not be feasible: perhaps the target rarely appears out in the open using his devices, or he is always covered by a bodyguard; perhaps physical interception poses too great a risk to officer safety; maybe the police are not willing to give away the existence of the investigation yet.

To get the plaintext, one option is for police to obtain the target’s passphrases, or the private encryption keys themselves. Law enforcement wants a way to get that information, without touching the target or his devices, from enough of a remove that they can operate safely and without giving their presence away. Their solution: conduct a side-channel attack to obtain the target’s private encryption key. Now the question arises: do they need a warrant? If so, and they do not get one, they risk exclusion of crucial evidence they see no other way to obtain.\(^\text{197}\) The next Section

---

\(^{195}\) This has happened at least twice. The operator of online black market the Silk Road, Ross Ulbricht, shielded his activities by using an encrypted instant messaging program and a full-disk encryption program for his laptop. FBI agents worked around those measures by apprehending him in October 2013 while he was sitting in a library with his laptop open. The agents created a distraction, then grabbed the laptop Ulbricht had been using moments before, pursuant to “orders . . . to seize the laptop in an open and unencrypted state.” Sarah Jeong, *The Dread Pirate’s Diary*, *Forbes* (Jan. 22, 2015, 12:14 AM), [http://www.forbes.com/sites/sarahjeong/2015/01/22/the-dread-pirates-diary/#1f634c8b37d3](http://www.forbes.com/sites/sarahjeong/2015/01/22/the-dread-pirates-diary/#1f634c8b37d3). More recently, Scotland Yard took a page from the FBI’s playbook when, late last year, undercover officers from the Metropolitan Police “mugged” a suspected credit-card fraudster on the street while he had his iPhone unlocked. Dominic Casciani & Gaetan Portal, *Phone Encryption: Police “Mug” Suspect to Get Data*, *BBC News* (Dec. 2, 2016), [http://www.bbc.com/news/uk-38183819](http://www.bbc.com/news/uk-38183819); see also *Encryption Workarounds*, supra note 60, at 24–26 (discussing these cases as examples of the “access plaintext when the device is in use” category of encryption workaround).

\(^{196}\) The option to compel the target to hand over his encryption keys or passphrases is an unsettled legal question, see *supra* Section II.B.3, and requires the investigation to have progressed far enough that police already have the suspect and his devices in custody, which has not yet happened in our hypothetical.

\(^{197}\) The exclusion of evidence obtained in violation of the Fourth Amendment is intended “to deter future Fourth Amendment violations.” United States v. Davis, 564 U.S. 229, 248 (2011) (citation omitted). Notably, there are significant limitations on the suppression remedy in the electronic-evidence context. Suppression is not an available remedy under the Stored Communications Act, 18 U.S.C. §§ 2708, 2712 (2012) or the Pen Register Act. United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014); United States v. Thompson, 936 F.2d 1249, 1250–51 (11th Cir. 1991). For Wiretap Act violations, suppression is available only as to wire and oral communications, not electronic...
addresses this question.  

III. APPLYING FOURTH AMENDMENT DOCTRINES TO SIDE-CHANNEL CRYPTANALYSIS

The courts have yet to define the Fourth Amendment’s scope when it comes to the sorts of intrusions implicated in side-channel attacks. These intrusions can occur without any physical interference, against computing devices not necessarily located within a home or office, to glean information that may or may not count as “content” information. Thus, the answer to the question of whether side-channel attacks require a warrant is every lawyer’s favorite phrase: it depends. This Section quickly reviews the Supreme Court’s two rubrics for Fourth Amendment analyses, then proceeds to analyze what legal process is required for a particular kind of side-channel attack—an electromagnetic key-recovery attack—by asking “what,” “where,” and “how.”

First, what side-channel information is law enforcement acquiring? What legal mechanism (if any) authorizes the seizure of encryption keys depends on whether the information counts as “content” information or “non-content” information.

Second, where is the side-channel information being acquired from? This Article assumes the information is being obtained from an “end point”: the targeted individual’s electronic device, i.e., a cell phone, tablet, laptop, or desktop computer. A device has the strongest privacy protection when it is inside the home, but a warrant may still be required for side-channel attacks against devices located outside the home.

Third, how is law enforcement acquiring the side-channel information? Side-channel attacks do not involve any physical trespass, but they measure emanations that are typically not detectable by human senses unaided. Kyllo v. United States supplies the rule for determining whether a warrant is needed: Did police use “sense-enhancing technology” “that is


198 This hypothetical fact pattern is admittedly abstruse. In the author’s defense, this is a law review piece—one that discusses computer security research, which rivals legal academia in its propensity for coming up with possible, but unlikely scenarios that have no bearing on the vast majority of situations that arise in the real world. See James Mickens, This World of Ours, USENIX (Jan. 2014), https://www.usenix.org/system/files/1401_08-12_mickens.pdf [https://perma.cc/Q7GE-FMTW] (“Unfortunately, large swaths of the security community are fixated on avant garde horrors . . . . [S]ecurity people need to get their priorities straight . . . . In the real world, threat models are much simpler.”). And after all, truth has a way of turning out to be stranger than fiction. See Jeong, supra note 195 (discussing the saga of the Dread Pirate Roberts).

199 The Article assumes that the “who” is U.S. law enforcement agents (federal, state, or local) investigating a U.S. citizen on U.S. soil for crimes unrelated to terrorism or national security, which are extremely complex areas of law out of scope of the Article.

not in general public use” to obtain information from a constitutionally-protected area?201 The Article proposes a set of factors for determining whether a technology is “in general public use,” then uses them to analyze various side-channel attacks.

The Section concludes by criticizing current Fourth Amendment jurisprudence, particularly the Kyllo “general public use” rule, as inadequate to protect Americans’ privacy rights from erosion by technological advances.

A. The Property-Based and Katz v. United States Approaches to the Fourth Amendment

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.”202 For a search or seizure to be reasonable, law enforcement generally (with certain exceptions) must first get a judicial warrant supported by probable cause.203

For half a century, in determining what counts as a “search” or “seizure” necessitating a warrant, courts have relied upon the “reasonable expectation of privacy” test first formulated in Justice Harlan’s famous concurrence in Katz v. United States.204 Under Katz, the Fourth Amendment is applicable only if the individual seeking its protection had a subjectively and objectively reasonable expectation of privacy that was invaded by the state’s action.205

The Katz test remains the courts’ “lodestar” when evaluating the constitutionality of “a particular form of government-initiated electronic surveillance.”206 But it is not the only test. Prior to Katz, the Court took an “exclusively property-based approach” to the Fourth Amendment, informed by the common law of trespass.207 Gradually, the Court came to understand that “property rights are not the sole measure of Fourth Amendment violations,”208 eventually proclaiming in Katz that “the Fourth Amendment protects people, not places.”209 That is, “a forbidden search can occur even when no trespass is involved.”210 The one rubric did not

---

201 Id. at 34–35, 40.
202 U.S. CONST. amend. IV.
204 389 U.S. 347 (1967).
205 Smith v. Maryland, 442 U.S. 735, 739–41 (1979) (citations omitted).
206 Id. at 739 (footnote omitted).
209 389 U.S. at 351.
replace the other: “the Katz reasonable-expectation-of-privacy test has been added to, not substituted for,” the property-centric test.211

In this century, the Supreme Court has called upon both tests when considering the constitutionality of particular forms of information-gathering by police. Yet the Court’s decisions have somewhat muddied the waters by focusing on the intrusions’ location in the sacrosanct space of the home in two of three major cases (Kyllo and Jardines), and, in the third (Jones), on another physical trespass on property. This complicates the task of predicting how courts will rule on future Fourth Amendment challenges to warrantless use of non-trespassory side-channel attacks.

B. What: Content versus Non-Content Information

What kind of information are police obtaining when they measure EM emissions in a side-channel key-recovery attack? The legal process required for an electromagnetic key-recovery attack depends on the characterization of an encryption key: does it qualify as content or non-content information? This is an open question as yet unaddressed by the courts, but it will be crucial when a court analyzes a key-recovery attack.

1. Are Encryption Keys “Content” or Not?

The courts212 and federal law213 both draw a distinction between “content” and “non-content” information. “Content” information means, basically, “a message that a person wants to communicate,” whereas “non-content” information can be characterized as “information about the communication that the [communications] network uses to deliver and process” the contents of the communication.214 If an encryption key

---

211 Jones, 565 U.S. at 409.
212 “The Supreme Court has . . . forged a clear distinction between” content information, which generally is entitled to Fourth Amendment protection (unless some exception applies), and non-content information, from which the Court has repeatedly chosen to “expressly withhold[]” Fourth Amendment protection.” United States v. Graham, 824 F.3d 421, 433 (4th Cir. 2016) (citations omitted). “Content” is not limited to communications; documents, i.e., personal papers that are not communicated to someone else, are also “content.” Id. at 434 n.13 (“[D]ocuments stored on phones and remote servers are protected, as ‘content,’ in the same way that the contents of text messages or documents and effects stored in a rented storage unit or office are protected.”) (citations omitted).
214 Orin Kerr, A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1228 (2004) (emphasis added; footnotes omitted) [hereinafter Kerr, User’s Guide]. ECPA affords greater privacy protections to content information than to non-content information “for reasons that most people find intuitive.” See id. (“Actual contents of messages naturally implicate greater privacy concerns than information (much of it network-generated) about those communications.”). However, the distinction between content and non-content information has become extremely blurry, as described in a recent article by several computer security experts. Steven M. Bellovin et al., It’s Too Complicated: How the Internet Upends Katz, Smith, and Electronic
qualifies as content information, then its seizure will typically require a warrant; not so if it is non-content information, though it may still be protected under some provision of ECPA.

Commentators disagree as to which definition best characterizes encryption keys. Some have argued that “[t]he encryption key has no communicative . . . content of its own but is merely a tool for deciphering the intercepted communication.” Lavabit took this stance in the Fourth Circuit, maintaining that its SSL keys were not “contents,” but “simply cryptographic tools . . . that convey neither meaning nor message.” A competing perspective counters that “when viewed in totality,” encryption keys should be treated like content information because they “change content from unreadable to readable text, thereby communicating information.” That is, the key’s functional aspect (scrambling or unscrambling text) does not extinguish its communicative properties. And a third view is that the answer depends on what kind of key is at issue. For example, a court could distinguish between an email system’s SSL keys and a particular user’s long-term identity key by finding that the latter

Surveillance Law, 30 HARV. J.L. & TECH. 1, 73–79 (2016); see also Mayer, supra note 116 (discussing how non-content metadata reveals a pattern of all our activities even without content information).

See Graham, 824 F.3d at 433; In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (“[c]ommunications content” requires a warrant, but addressing and routing information do not) (citing Smith v. Maryland, 442 U.S. 735, 741 (1979), United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008)).

See United States v. Walker, No. 16-cr-567 (JSR), 2017 U.S. Dist. LEXIS 38102, at *8 (S.D.N.Y. Mar. 8, 2017) (Title II of ECPA, the Stored Communications Act, largely draws distinctions that “track the rule that the contents of communications are generally protected by the Fourth Amendment, whereas information principally used in transmitting the information is generally not,” with some exceptions) (citing United States v. Carpenter, 819 F.3d 880, 886–87 (6th Cir. 2016), cert. granted, 85 U.S.L.W. 3569 (U.S. June 5, 2017) (No. 16-402)). Of course, state laws and constitutions also protect the privacy of content and non-content information, sometimes more so than their federal counterparts; however, they are out of scope of this Article. See, e.g., Susan Freiwald, At the Privacy Vanguard: California’s Electronic Communications Privacy Act (CalECPA), 33 BERKELEY TECH. L.J. (forthcoming 2018), https://papers.ssm.com/sol3/papers.cfm?abstract_id=2939412 [http://perma.cc/KE75-VPQC] (describing how a new California statute “improves upon” ECPA in its “expansiveness and its additional protections”).


Wilson, Compelling Passwords, supra note 116, at 21 & n.112 (acknowledging “the uncertainty of whether passwords [and keys] are content or non-content data”). The article uses the term “password” to include “encryption keys.” Id. at 3 n.1.

See Bernstein, 176 F.3d at 1141–42 (holding that encryption software source code’s functional aspects could not “overwhelm[ ] any constitutional protections that expression might otherwise enjoy”).
communicates that the user is who she claims to be and the message she is sending is authentic,221 while the former communicate nothing.

Given these conflicting arguments, it is not clear how a court would rule in a case involving the seizure of private encryption keys. If the court deems them to be non-content information, then as said, the Fourth Amendment does not require police to get a warrant, although some form of process may be required by statute.222 If the court holds that the keys are content information, that does not end the analysis: the court still must ask where and how police conducted the key-extraction attack.

2. What Legal Process Authorizes the Seizure of Encryption Keys?

Whether encryption keys are content or non-content guides what legal process (if any) is required to seize them. When investigators seek a target’s encryption keys in order to access evidence in plaintext, “finding the key often requires the legal authority to search for and seize it.”223 For the seizure of encryption keys, that legal authority is not clear-cut, and which authority applies requires careful examination of exactly what it is that law enforcement wishes to seize.

a. Search Warrants

---

221 See Felten, supra note 21, at 3, 4 (“A party can use its long-term identity key to prove its identity to other parties,” and a malicious actor who learns that key could impersonate the user).

222 See supra notes 205–12 and accompanying text. The Supreme Court has held that the Fourth Amendment also affords no protection to “information [someone] voluntarily turns over to third parties.” Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435 (1976). The third-party doctrine should not apply to private encryption keys. A user’s private device and long-term identity keys are not transmitted to third parties. See supra notes 21, 22 and accompanying text. Session keys for encrypting messages are exchanged only between the two parties to the communication. See Felten, supra note 21, at 3 (session keys are “known only to the two of them”). That is, they are not disclosed to the encrypted communications service provider. “Without a third party, the third party doctrine is inapplicable.” United States v. Lambis, 197 F. Supp. 3d 606, 614–16 (S.D.N.Y. 2016) (unlike cell-site location information “pings” voluntarily transmitted by phones to cell network, location information involuntarily transmitted by phone directly to government’s cell-site simulator was not subject to third-party doctrine).

The Lavabit case is not to the contrary. Lavabit architected its service so that it held the “single set of [private and public] SSL keys for all its various subscribers.” In re Under Seal, 749 F.3d 276, 280 (4th Cir. 2014). Lavabit’s users “never had access to those private keys.” Lavabit Brief, supra note 218, at 22. That is, Lavabit was not a “third party” to whom its users turned over their private keys. And anyway, there is no need to resort to a side-channel attack if a provider holds the encryption keys police seek. As they did with Lavabit, police can try to demand the keys directly from the service provider. That implicates different legal issues than does seizure from the user. See Encryption Workarounds, supra note 60, at 15–16; see generally When the Cops Come A-Knocking, supra note 149 (reviewing law enforcement’s authority to demand various kinds of information or assistance from third-party service providers).

223 Encryption Workarounds, supra note 60, at 11.
The Fourth Amendment permits warrants to issue only upon probable cause\textsuperscript{224} to believe that the search will turn up “fruits, instrumentalities, or evidence of a crime.”\textsuperscript{225} Federal Rule of Criminal Procedure 41, which governs the issuance of warrants, enumerates similar categories of property subject to search and seizure.\textsuperscript{226}

Encryption keys do not fit comfortably within these categories. In appealing a seizure warrant, encrypted email service provider Lavabit\textsuperscript{227} argued that there was no probable cause to seize its private SSL encryption keys.\textsuperscript{228} Its keys were not fruits, instrumentalities, evidence (either of a crime or for impeachment), or contraband.\textsuperscript{229} Nor are encryption keys designed or intended for criminal use: encryption programs are legal and general-purpose.\textsuperscript{230} There is thus an argument that the Fourth Amendment and Rule 41 do not authorize the seizure of encryption keys.\textsuperscript{231}

All the same, Lavabit’s facts will not apply in every case. Depending on the specific facts presented in a warrant application, a court might decide that even if an encryption key is not evidence, fruit, or contraband, it is an instrumentality of a crime (e.g., possession of child pornography), and conclude that seizure with a warrant is proper.\textsuperscript{232} The government, for its part, appears to find the propriety of a warrant to be uncontroversial: the DOJ’s model electronic-evidence warrant includes encryption keys in the

\textsuperscript{224} U.S. CONST. amend. IV.
\textsuperscript{226} FED. R. CRIM. P. 41(c) (authorizing the search or seizure only of property that is “evidence of a crime,” “contraband, fruits of a crime, or other items illegally possessed,” or “designed for use, intended for use, or used in committing a crime”). We assume a federal investigation governed by federal procedural rules because side-channel attacks are more likely to be the province of federal investigators than of state or local authorities. See Encryption Workarounds, supra note 60, at 30, 33–35.
\textsuperscript{227} See supra Section II.B.3.
\textsuperscript{228} Lavabit Brief, supra note 218, at 20–24; see also When the Cops Come A-Knocking, supra note 149 (noting, in slides 23 through 25, that encryption keys are not evidence of a crime or contraband, discussing the Lavabit seizure warrant, and concluding that it is unknown whether a warrant can be used to compel keys’ disclosure to police).
\textsuperscript{229} Id. at 20, 22–23 (citing Zurcher, 436 U.S. at 549–50). The Fourth Circuit declined on procedural grounds to rule on the merits of this argument. In re Under Seal, 749 F.3d at 285–86.
\textsuperscript{230} See supra Section II.A.
\textsuperscript{231} Cf. In re Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006) (holding that the Fourth Amendment and Rule 41 require “probable cause to believe that the information sought is itself evidence of a crime,” not that it is merely “relevant to an investigation” or “can be expected to produce admissible evidence”). This opinion has been critiqued for “read[ing] more into Rule 41 than was intended.” In re Application of the U.S. of Am., 727 F. Supp. 2d 571, 581 (W.D. Tex. 2010).
\textsuperscript{232} Cf. United States v. Scarfo, 180 F. Supp. 2d 572, 577–78, 581 (D.N.J. 2001) (upholding investigators’ use of keystroke logger, which “was devised by F.B.I. engineers using previously developed techniques in order to obtain a target’s key and key-related information,” to get passphrase to encrypted computer file) (discussed in Encryption Workarounds, supra note 60, at 10–11).
sample list of items to be seized.\footnote{U.S. Dep’t of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, EXEC. OFF. FOR U.S. ATT’YS 1 app. at 249 (2009).}

b. \textit{ECPA}

ECPA is the federal statutory framework that primarily governs electronic surveillance.\footnote{Since ECPA’s enactment, “electronic surveillance has been governed primarily, not by decisions of [the Supreme] Court, but by the [ECPA] statute, which authorizes but imposes detailed restrictions on electronic surveillance.” Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring).} It provides several means for law enforcement to obtain “content” information about communications. The Wiretap Act (Title I of ECPA) governs seizures of the contents of “electronic communications” in transit;\footnote{18 U.S.C. § 2516 (2012).} the Stored Communications Act (SCA) (Title II of ECPA) governs seizures of contents in electronic storage.\footnote{Id. § 2703(a), (b).}

It is questionable whether these provisions should apply to seizure of encryption keys. Private keys arguably do not count as “electronic communications” or “contents” thereof. An “electronic communication” entails a “transfer” of information over a “system that affects interstate or foreign commerce” (such as the internet).\footnote{Id. § 2510(12) (“[E]lectronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce”). \textit{See also id.} § 2510(8) (“contents” of a wire, oral, or electronic communication means “any information concerning the substance, purport, or meaning of that communication”).} But private encryption keys should never be transmitted over such a system.\footnote{See supra notes 21, 22 and accompanying text.} And an individual’s computer or smartphone is not itself such a “system,” even if it connects to one.\footnote{United States v. Ropp, 347 F. Supp. 2d 831, 837–38 (C.D. Cal. 2004) (noting the Act’s definition of “electronic communications” applies only to data that is in fact being transmitted beyond a local computer by a system that affects interstate commerce).} Lavabit raised this argument in its appeal, but the Fourth Circuit did not reach its merits, leaving the issue undecided.\footnote{\textit{In re} Under Seal, 749 F.3d 275, 285–86 (4th Cir. 2014). Lavabit contended that the SCA did not authorize a warrant to seize its private SSL keys on the grounds they were not “electronic communications” under ECPA, since there is never any “transfer” or “transmission” of Lavabit’s private keys. Lavabit Brief, \textit{supra} note 218, at 18–19.}

On the other hand, the exchange of session keys for encrypting communications \textit{does} entail such a system, making that exchange look like an “electronic communication.”\footnote{See Felten, \textit{supra} note 21, at 3.} A court might conclude that it is, but that session keys are \textit{not} content information. If so, it could authorize the side-channel seizure under the Pen Register Act (Title III of ECPA)—provided it also finds that session keys count as “dialing, routing,
addressing, or signaling information.”242 This seems doubtful: the purpose of a session key is to protect a message’s confidentiality and integrity.243 It not help deliver the message it encrypts. If the court concluded, though, that the session keys are “contents,” it could then authorize a wiretap order allowing the interception of session keys as they are being exchanged between the target and the target’s interlocutor.244

In sum, the content/non-content distinction is a crux of the legal analysis of an electromagnetic key-extraction attack, and courts must carefully consider the particular type(s) of encryption key sought to be seized.245

C. Where: Side-Channel Attacks and Constitutionally-Protected Areas

A Fourth Amendment analysis of a side-channel attack must also take into account where the end point being targeted is located and where the police (and their equipment) are located. The modern understanding of the Fourth Amendment since Katz is that it “protects people, not places.”246 Nevertheless, the property-based understanding of the Fourth Amendment remains a viable doctrine, available whenever the police accomplish a trespassory intrusion on privacy.247

The Supreme Court’s application of the property-based and Katz doctrines has been confusing. The home has always held a special place in Fourth Amendment jurisprudence, making it the “most commonly litigated

242 18 U.S.C. §§ 3123, 3127(3) (defining “pen register” as “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication”).

243 See Felten, supra note 21, at 3, 4.

244 18 U.S.C. § 2516 (authorizing interception of electronic communications); id. § 2510(4) (“‘[I]ntercept’ means 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.”).

245 Content/non-content distinctions among different types of encryption keys could create practical headaches for investigators. An electromagnetic side-channel key-extraction attack could putatively sweep in several kinds of key; if some are “content” and others not, investigators risk exceeding the authorization issued by the court. For example, a pen register order does not allow the collection of content information. See id. § 3127(3). A court challenge might necessitate an in-depth analysis of how the attack worked, how the attack equipment was configured, and exactly what information it did or did not collect. See Scarfo, 180 F. Supp. 2d at 575, 581–82 (carefully analyzing whether keystroke logger intercepted wire communications, where agents had obtained search warrants but not a wiretap order). Out of caution, investigators who do not know beforehand what information their side-channel attack will yield might choose to apply for a wiretap order, despite the heightened showing this would require. See In re Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 753 (S.D. Tex. 2005) (setting forth ECPA’s four broad categories of electronic surveillance, “arranged from highest to lowest legal process for obtaining court approval”).


area of protected privacy.” In its “incoherent” jurisprudence on cases involving “sense-enhancing” surveillance, the Court appears to apply “a more searching review” to techniques that intrude on the home than to those that do not. More generally, whether a physical trespass occurred “often seems determinative” in these cases.

In Kyllo v. United States and the more-recent Florida v. Jardines, the Court found warrantless searches of the home using sense-enhancing “devices” to be unconstitutional. In both cases, the home seemed to be the dispositive factor, regardless of which rubric—Katz or property—the Court was nominally applying. Similarly, in United States v. Jones, the Court held unconstitutional the warrantless use of a GPS device affixed to a vehicle—because it intruded on property. Jones clarified that the Katz analysis applies to non-trespassory electronic surveillance, but left for another day how the Fourth Amendment would play out in the case of a non-trespassory intrusion upon privacy interests outside of the home.

This lack of guidance complicates the task of analyzing the use of side-channel key-recovery attacks against end-point devices. A warrant is typically required when police monitor electronic devices that are inside a home, but Kyllo creates an exception. Outside the home, a warrant may also be required, but arriving at that answer is not straightforward. How the attack is conducted proves highly important in both situations.

1. Side-Channel Attacks Against Devices in Constitutionally-Protected Areas

The Fourth Amendment “protects people, not places.” Nevertheless, the law places the home at the apex of Fourth Amendment protection. In Kyllo v. United States, the Supreme Court held that when law enforcement agents use “sense-enhancing technology” to measure emissions from a

---

249 David E. Steinberg, Sense-Enhanced Searches and the Irrelevance of the Fourth Amendment, 16 WM. & MARY BILL RTS. J. 465, 467–70 (2007) [hereinafter Steinberg]. Steinberg argued that “the Fourth Amendment has no applicability to the vast majority of sense-enhanced searches” and that the Supreme Court’s “arbitrary and inconsistent” decisions in such cases underscore the need for this area to be regulated instead by statute. Id. at 466–67.
250 Steinberg, supra note 249, at 468.
254 Id. at 404, 412.
255 Id. at 411.
256 Id. at 412.
home, they must get a warrant. That rule applies to side-channel attacks on devices that are located inside homes, and should extend to devices in similar constitutionally-protected spaces such as offices as well.

In *Kyllo*, federal agents had warrantlessly used a thermal imaging device to scan the Kyllo home from their position on a public street. The Court ruled the scan an unconstitutional warrantless search. While applying *Katz*, the Court also emphasized the “firm,” “bright” line the Fourth Amendment draws around the home. It held that “obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’ . . . constitutes a search—at least where . . . the technology in question is not in general public use.” In an age of rapid technological change, the Court observed, the nation’s federal courts must be prepared to prevent police technology from eroding the Fourth Amendment’s privacy guarantees.

*Kyllo* also held that the “made public” and “plain view” doctrines did not foreclose Fourth Amendment protection. Generally, the Fourth Amendment does not protect “[w]hat a person knowingly exposes to the public, even in his own home or office.” *Kyllo* rejected the application of this doctrine to waste heat emitted from a home, upending several appellate-court decisions to the contrary. It also rejected the applicability of the “plain view” doctrine, which applies to contraband left in plain view or discarded trash set out by the curb, to a home’s waste heat emissions.

Subsequently, in *Florida v. Jardines*, the Court held unconstitutional a warrantless drug dog sniff on a defendant’s front porch. The Court again

---

259 Id. at 34; Florida v. Jardines, 133 S. Ct. 1409, 1419, 1425 (2013).
261 Id. at 34–35.
262 Id. at 34–35, 40.
263 Id. (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).
264 Id. at 34 (courts must define “what limits there are upon th[e] power of technology to shrink the realm of guaranteed privacy,” and must not “permit police technology to erode the privacy guaranteed by the Fourth Amendment”).
266 United States v. Kyllo, 190 F.3d 1041, 1046 (9th Cir. 1999) (collecting cases from the Fifth, Seventh, Eighth, and Eleventh Circuits), rev’d, 553 U.S. 27 (2001). The four-justice dissent in *Kyllo* took this position as well, contending that a thermal-imaging device merely captures heat “waves emanating from a private area into the public domain.” 553 U.S. at 49 (Stevens, J., dissenting). The majority rejected this “mechanical interpretation of the Fourth Amendment” as inconsistent with *Katz*, wherein “the eavesdropping device picked up only sound waves that reached the exterior of the phone booth.” Id. at 35.
267 Id. at 37–38 (residence’s warmth was an “intimate detail[] of the home”); see also id. at 42–43, 44 (Stevens, J., dissenting) (citing California v. Greenwood, 486 U.S. 35, 40–41 (1988) & Payton v. New York, 445 U.S. 573, 586 (1980)).
stressed the Fourth Amendment primacy of the home and its curtilage. But unlike in Kyllo, the Court based its decision not on Katz, but on the property-based rubric of the Fourth Amendment. Thus, the longstanding police use of drug-sniffing dogs as a “‘sense-enhancing’ tool” was not determinative; rather, the physical intrusion onto property was key.

Kyllo and Jardines both involved the home, but they need not be limited to it. The Fourth Amendment requires a warrant to search someone’s office or hotel room, too. That is because, although the home is “first among equals,” the Fourth Amendment nevertheless “safeguard[s] individuals from unreasonable government invasions of legitimate privacy interests, and not simply those interests found inside the four walls of the home.” Accordingly, police obtain warrants when they wish to search or seize computers from the constitutionally-protected spaces of offices and hotel rooms. That is consistent with both the trespass-based approach to the Fourth Amendment (relied on in Jardines) and the Katz reasonable-expectation-of-privacy framework (relied on in Kyllo). Therefore, despite the two cases’ confusing emphasis on the special role of the home, this Article assumes that a court would extend Kyllo and Jardines to the constitutionally-protected spaces inside offices and hotel rooms.

---

269 Id. at 1414, 1417–18 (home is “first among equals” under the Fourth Amendment).
270 Id. at 1414 (property-based approach “renders this case a straightforward one”).
271 Id. at 1417, 1419 (quoting Kyllo, 533 U.S. at 40).
272 Id. at 10–11 (citing United States v. Jeffers, 342 U.S. 48 (1951) (hotel room); G.M. Leasing Corp. v. United States, 429 U.S. 338 (1977) (office); Mancusi v. DeForte, 392 U.S. 364 (1968) (office)).
273 Jardines, 133 S. Ct. at 1414.
274 United States v. Chadwick, 433 U.S. 1, 10–11 (1977) (citations and footnote omitted) (listing spaces requiring a warrant to search, including sealed packages and envelopes sent through the mail, public phone booths, hotel rooms, offices, and automobiles on private premises or in police custody), abrogated on other grounds by California v. Acevedo, 500 U.S. 565 (1991).
275 See United States v. Pirosko, 787 F.3d 358, 362–63 (6th Cir. 2015) (federal agents executed a search warrant on defendant’s hotel room and seized a laptop computer, which defendant had used to share child pornography over peer-to-peer networks that he accessed online from hotel rooms across the country); Scarfo, 180 F. Supp. 2d at 574 (police obtained warrants to enter Scarfo’s business office and install a keylogger on his computer there).
276 See Jeffers, 342 U.S. at 51–52 (holding, pre-Katz, that warrantless search of hotel room violated its occupants’ Fourth Amendment rights; because the occupants “were not even present when the entry, search and seizure were conducted,” the agents’ “intrusion was conducted surreptitiously and by means denounced as criminal”).
277 A hotel guest has a reasonable expectation of privacy in her hotel room. Stoner v. California, 376 U.S. 483, 490 (1964).
278 The Fourth Circuit, in an unpublished opinion examining the constitutionality of a drug dog sniff in the hallway outside the unfortunately-named defendant Legall’s hotel room, rejected both a Jardines argument that the hallway was within the curtilage of the hotel room and, consequently, a Kyllo argument that the trained drug-sniffing dog was a “device not in general public use” that infringed on his legitimate expectation of privacy. United States v. Legall, 585 F. App’x 4, 5–6 (4th Cir. 2014) (per curiam) (citing Illinois v. Caballes, 543 U.S. 405, 409, 410 (2005)). On that rationale,
Kyllo and Jardines apply readily to law enforcement side-channel attacks when the targeted electronic device is in someone’s home or office. Devices’ EM emissions and the equipment to measure them are comparable to the waste heat and thermal-imaging device in Kyllo.279 EM emissions happen without any volitional action, or probably even awareness, on the device owner’s part, meaning they are not “knowingly exposure[d] to the public”280 and do not fit the “plain view” standard. Even if she knows about the emissions, the device’s owner may reasonably expect that “‘observ[ing]’ [EM emissions] emanating from [the device] requires sophisticated equipment that a trash picker probably does not have.”281

In short, under Kyllo, when a device in a home or office throws off EM emissions into the open air, it is “not determinative” for Fourth Amendment purposes “that information is made publicly available, at least where access requires technology”—as recovering encryption keys from EM emissions assuredly does.282

Consequently, the use of EM emission-measuring equipment against a device inside a home or office indisputably requires a warrant if police physically intrude on the property to conduct the attack, as in Jardines (because the property rubric applies). If the device is inside a protected space but police carry out the side-channel attack from a public vantage point (i.e., without a physical trespass), Kyllo and the Katz test require them to get a warrant—unless the police’s device is in general public use, a variable explored in Section III.E below.283

2. Side-Channel Attacks Against Devices Outside of Protected Areas

Kyllo and Jardines demonstrate that both Fourth Amendment rubrics can protect privacy interests inside the home. What, then, is the proper test when police conduct a non-trespassory side-channel attack to measure the narrow hallways in hotels or office buildings might be a boon to law enforcement agents conducting side-channel attacks, as a thin or nonexistent curtilage is compatible with the very close proximity that electromagnetic side-channel attacks presently require.


283 For now, the physical-trespass situation is more likely. As described earlier, EM key-recovery attacks presently work only at very close distances, meaning the sensing equipment likely would need to be located right up against the wall of the home. See supra notes 35–40 and accompanying text. Law enforcement agents would have to either be on the property during the attack, or at least enter onto it in order to place their equipment there before retreating off the property to carry the attack out.
emissions from an electronic device that is not in a protected space such as the target’s home or office (e.g., a laptop in use in a cafe)? The Supreme Court has stated that the Katz “reasonable expectation of privacy” test applies to non-trespassory electronic surveillance. Kyllo’s “sense-enhancing technology not in general public use” rule should extend to this context, too, though the Court has not clarified whether it does so.

a. The Katz Framework Applies to Non-Trespassory Side-Channel Attacks

The 2012 Supreme Court case United States v. Jones clarified that the Katz rule governs novel “nontrespassory surveillance techniques” for search and seizure of information. In Jones, police physically mounted a GPS tracking device on a vehicle and tracked its movements for 28 days. The Court unanimously agreed that this was a search, but not why.

The majority opinion based its reasoning on the GPS installation’s physical intrusion on the defendant’s “effect”—the vehicle. It applied the property-based Fourth Amendment rubric, vigorously rejecting the idea that the Katz test had replaced it. In concurring opinions, multiple justices expressed doubts about the property-based rubric’s applicability in situations of non-trespassory electronic surveillance.

Jones establishes that the Katz “reasonable expectation of privacy” framework applies to the novel non-trespassory electronic surveillance method of electromagnetic key-extraction attacks. Therefore, if a device’s

---

285 Id. at 953–54; see also id. at 955 (Sotomayor, J., concurring).
286 Id. at 948–49.
287 Id. at 949. Compare id. at 954 (majority opinion) (the installation of a GPS device on a target’s vehicle constituted trespass, and therefore a physical intrusion), with id. at 954 (Sotomayor, J., concurring) (arguing that the Government obtained personal information without a valid warrant and without the respondent’s consent, and therefore invaded the respondent’s property interests), and id. at 964 (Alito, J., concurring) (opining that the lengthy monitoring of vehicle’s movements violated the defendant’s reasonable expectations of privacy).
288 Id. at 949 (internal quotation marks omitted).
289 Id. at 950–51, 953.
290 Justice Alito’s concurring opinion pointed out that the majority’s trespass-based framework did not adequately account for “cases involving surveillance that is carried out by making electronic, as opposed to physical, contact.” Id. at 962 (Alito, J., concurring). Justice Sotomayor agreed with him, cautioning in her own separate concurrence that the trespass rubric would be of little help in cases involving “electronic or other novel modes of surveillance that do not depend upon a physical invasion on property.” Id. at 955 (Sotomayor, J., concurring).
291 Id. at 953; see also id. at 954 (“We may have to grapple with these ‘vexing problems’ in some future case where a classic trespassory search is not involved and resort must be had to Katz analysis; but there is no reason for rushing forward to resolve them here.”) (internal quotation omitted).
owner has a reasonable expectation of privacy in the information revealed by the device’s EM emissions, then a non-trespassory side-channel attack on those emissions will require a warrant.292

b. Privacy Protections for Electronic Devices and Their Contents

The Fourth Amendment is not read narrowly to protect only “the catalog (‘persons, houses, papers, and effects’)” of categories its text enumerates.293 “[E]ffects” encompasses the closed containers that hold them.294 Computers and smartphones are analogous (if imperfectly) to containers as electronic “repositor[ies] of personal effects.”295 Several appeals courts have extended the “container” analogy to computers,296 finding them generally subject to a reasonable expectation of privacy.297

In addition, the amount and sensitivity of the personal information in those “containers” gives rise to an independent layer of protection for that data, even if an exception applies that would otherwise subject the container to a warrantless search. Because our cell phones provide “a digital record of nearly every aspect of [our] lives,” the Supreme Court held in Riley v. California that a warrant is required for searches of cell phones incident to arrest.298 Ordinarily, closed containers found on an arrestee’s person may be searched without a warrant.299 But our phones are not like other “containers,” an analogy the Court viewed skeptically.300

294 United States v. Chadwick, 433 U.S. 1, 11 (1977) (holding that a warrant was needed to search a locked footlocker, because someone who manifests an expectation of privacy by “placing personal effects inside a double-locked footlocker” is entitled to Fourth Amendment protection “[n]o less than one who locks the doors of his home against intruders”).
295 Id. at 13.
296 E.g., United States v. Andrus, 483 F.3d 711, 718–19 (10th Cir. 2007) (deciding to categorize computers alongside suitcases and footlockers); Trulock v. Freeh, 275 F.3d 391, 402–04 (4th Cir. 2001) (analogizing password-protected files on a shared computer to the footlocker in Chadwick).
299 Id. at 2483–84 (citing Chadwick, 433 U.S. at 15; United States v. Robinson, 414 U.S. 218 (1973)).
300 Riley, 134 S. Ct. at 2491 (calling analogy “a bit strained”). At worst, the Court thought the analogy wholly inapt with regard to data that police view locally on a phone but that is stored remotely in the cloud. Id. The prevalence of cloud storage illustrated the analogy’s shortcomings: containers may be searched incident to arrest, but Riley established that electronic devices are not subject to that exception, in part because of the possibility that some information that is viewable on a phone is in fact stored remotely. Id. The Court’s recognition of the container analogy’s limitations is noteworthy and laudable. Unfamiliar technologies may prompt judges to draw analogies to the familiar physical
Rather, it concluded that police must get a warrant due to the “broad array of private information” our cell phones reveal about us.301

In short, people generally have a reasonable expectation of privacy against the warrantless search and seizure of their electronic devices and the information they contain, irrespective of whether the device is located inside or outside the home.302

c. Extending the Kyllo Rule to Side-Channel Attacks on Devices Outside Constitutionally-Protected Areas

In an electromagnetic key-recovery attack, agents seize an encryption key by measuring side-channel information emitted by an electronic device, without physically seizing the device to obtain information from it. Such non-trespassory surveillance is evaluated under the Katz “reasonable expectation of privacy” framework.303 There is generally a reasonable expectation of privacy against warrantless electronic surveillance of devices and their contents.304 Since a device’s owner has a reasonable expectation of privacy in the device and the information its EM emissions reveal, it follows that a non-trespassory side-channel attack should generally require a warrant, no matter where the device is located.

However, under Kyllo, police must get a warrant to use “sense-enhancing technology” such as side-channel attack equipment only if the device is not “in general public use”—at least as to surveillance of the home.305 Should this rule extend to EM side-channel attacks against devices in a public place, which involve no intrusion into the home or seizure of the device itself?

On the one hand, it is challenging to know how to apply Kyllo outside the home. The opinion focuses heavily on the home, but not in a

---

301 Riley, 134 S. Ct. at 2491, 2485 (“[Cell phones] place vast quantities of personal information literally in the hands of individuals”), 2494–95 (“[w]ith all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’”) (citation omitted).

302 This expectation does not turn on whether the device’s owner “locks” it by encrypting and/or password-protecting it. Such measures’ legal effect is unsettled. Compare Trulock, 275 F.3d at 403 (“By using a password, Trulock affirmatively intended to exclude [the computer’s other user] and others from his personal files. . . . Trulock had a reasonable expectation of privacy in the password-protected computer files and . . ., therefore, has alleged a violation of his Fourth Amendment rights.”), with Rozenshtein, supra note 61, at *30 (“one scholarly debate asks whether merely encrypting a communication is enough to raise a reasonable expectation of privacy in it, thus triggering Fourth Amendment protections”) (citing Orin S. Kerr, The Fourth Amendment in Cyberspace: Can Encryption Create a “Reasonable Expectation of Privacy?” , 33 CONN. L. REV. 503, 505 (2001) (posing that “encryption cannot create Fourth Amendment protection”)).

303 See supra Section III.C.2.a.

304 See supra Section III.C.2.b.

particularly coherent way that would guide its application outside that context. Professor Henderson believes that Kyllo’s fixation on the home and its special role, while failing to engage directly with the legal consequences (under the third-party doctrine) of Kyllo’s failure to block the radiation emanating from his home, “renders the entire opinion of questionable significance outside the context of the home.”

Yet there is a strong argument that Kyllo should extend to side-channel attacks that measure EM emissions from devices in public spaces. This seems intuitively correct given that Kyllo itself involved the measurement of side-channel information. A side-channel attack on an electronic device in public is like the thermal imaging of the Kyllo home: it is a non-trespassory intrusion, conducted from a public vantage point, to measure information that is protected as private, from something that is constitutionally protected (the container-like electronic device here, the home in Kyllo).

Further, if we apply the Katz “reasonable expectation of privacy” test (as Kyllo did and as Jones requires), Katz itself is also closely analogous. A device that collects EM emissions radiated from a target’s computer or cell phone in public is similar to the eavesdropping device that picked up sound waves emitted from the phone booth in Katz. It did not matter to the Court that Katz made his calls from a glass-walled phone booth in public: “the Fourth Amendment protects people, not places,” so it “nonetheless protected Katz from the warrantless eavesdropping because he ‘justifiably relied’ upon the privacy of the telephone booth.”

Just as someone who goes into a phone booth and closes the door behind him before placing a call “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,” someone discreetly using a laptop or cell phone in public may reasonably

---


307 See Kyllo, 533 U.S. at 29 (“infrared radiation, which virtually all objects emit but which is not visible to the naked eye”).

308 Private encryption keys, which a court could deem particularly sensitive in keeping with Riley’s concern with not just the quantity, but also the sensitive quality of the information that our electronic devices hold about us. See Riley, 134 S. Ct. at 2490 (“[C]ertain types of data are also qualitatively different.”). A court might view encryption keys as especially sensitive information because encryption is what protects from snooping eyes the other kinds of private and sensitive information that concerned the Riley Court. See id. (listing, e.g., Internet browsing history revealing searches for disease symptoms, and apps that would reveal political and religious affiliations, addiction, pregnancy, and personal budget details).

309 See Kyllo, 533 U.S. at 35–36.


311 Kyllo, 533 U.S. at 32–33 (citing Katz, 389 U.S. at 353).

312 Katz, 389 U.S. at 352.
expect that police are not surreptitiously spying on that usage. This is
doubly true of the electromagnetic emissions that reveal encryption keys.
Even if a cell phone’s user could not reasonably expect his WhatsApp
phone call to remain private if he conducted it loudly on speaker-phone
while strolling down the main thoroughfare, this behavior (though
obnoxious) does nothing to expose the app’s secret encryption keys to the
public. Those, he may reasonably expect will remain private.

Extending Kyllo to spaces outside the home also avoids an absurd
result. Kyllo creates an exception to the warrant requirement for use of
sense-enhancing technology to measure otherwise-private information
about the interior of a home, where the technology is “in general public
use.” But as noted, people generally have a reasonable expectation of
privacy in their cell phones and laptops wherever they may be. It would
make little sense for a device to be subject to the Kyllo exception while it is
inside the home, where the Fourth Amendment’s protection is supposedly
at its zenith, but receive more robust protection once it leaves the home.

Kyllo’s “general public use” rule thus should extend to side-channel
attacks against devices when they are in public spaces, not just in the
home. Adapted for electronic devices, the Kyllo test reads: where the
government uses sense-enhancing technology that is not in general public
use, to explore details of an electronic device that would previously have
been unknowable without a physical intrusion into the device, the
surveillance constitutes a “search” and is presumptively unreasonable
without a warrant.

An electromagnetic key-recovery attack seeks to learn information for
purposes of extracting private keys from an electronic device (and,
ultimately, obtaining plaintext using the extracted keys). That information
“would previously have been unknowable without physical intrusion”,
that is, direct physical access to the device—hence the need for a side-
channel attack. Accordingly, if the side-channel attack uses a sense-
enhancing device that is not in general public use, the police must get a
warrant. If the device is in general public use, no warrant is necessary. The
next Section delves into the “general public use” analysis.

E. How: Analyzing Sense-Enhancing Side-Channel Key-Recovery
Equipment under the Kyllo “General Public Use” Test

Just how law enforcement agents carry out a side-channel attack is a
critical final step in the Fourth Amendment analysis. Stated simply, when

---

313 Kyllo, 533 U.S. at 34.
314 See id. at 34, 40.
315 Id. at 40.
316 See supra Section II.D.
the how of non-trespassory surveillance means using a “sense-enhancing technology” that is “not in general public use,” Kyllo says the police must get a warrant. In announcing this rule, the Court strove to “take the long view” of the Fourth Amendment in light of technological advances. It refused to “leave the homeowner at the mercy of advancing technology,” noting that while the thermal imaging device at issue “was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development. Nevertheless, the rule Kyllo announced is very fact-dependent, and its outcome can change over time as society acclimates to new technologies. Attacks that measure side-channel information such as minute vibrations, sounds inaudible to the human ear, or electromagnetic emissions not on the visible spectrum, indisputably require “sense-enhancing” equipment. But yesterday’s “sophisticated system” is tomorrow’s “crude” tool. That is, a device that was “not in general public use” at the time Kyllo was decided would not necessarily still qualify as such today, and what qualifies today may come into “general public use” in the future.

1. What Makes a Device “in General Public Use”? The side-channel attack technologies discussed in Section I doubtless enhance the human senses under Kyllo. But not every “sense-enhancing technology” is “not in general public use.” What, then, makes a device “in general public use”? Commentators have suggested several factors to be taken into account: cost, availability, legal restrictions, consumer choice, and social norms.

According to commentator Stephen A. LaFleur, “[g]eneral public use is a function of cost, availability, and the lack of statutory restrictions on possession.” These factors are intertwined: “[g]iven the cost trends in consumer electronic devices,” greater affordability of a device will lead to greater availability, but “government restriction” will hinder availability.

Professor Stephen E. Henderson suggested factors akin to LaFleur’s, but added social norms. The Kyllo “general public use” test, intersecting as it does with the Katz “reasonable expectation” test, refers to what behaviors society considers normal and expected, not what behaviors are

317 Kyllo, 533 U.S. at 34.
318 Id. at 40.
319 Id. at 35–36 (footnote omitted).
320 Professor Steinberg points out that the sense the thermal-imaging device amplified in Kyllo by measuring infrared radiation was that of touch (to detect heat), not sight. Steinberg, supra note 249, at 469–70.
321 LaFleur, supra note 281, at 945.
322 Id.
323 Henderson, After Jones, supra note 282, at 440, 445.
possible. That is, Kyllo “look[s] not to what persons could do, but to what they actually do.”

324 What behavior is normal, though, is determined in part by statutory strictures, i.e., “what the law permits and prohibits.”

325 Thus, whether a device is “in general public use” “will depend not solely upon developments in technology and consumer choice, but also upon any statutory restrictions on the sale or use of such devices.”

Cost, legality, and availability are clearly fundamental, as Professor Henderson and LaFleur agree. But “availability” and “social norms” are concepts with some subtlety to them. For example, “community band” (CB) radios are available from Radio Shack, but they are used mainly by truckers; most people nowadays just use cell phones. Yet thanks to Smokey and the Bandit, the general public knows about CB radios.

Consequently, even if a device is only “in general public use” within a particular market or community (anymore), the general public’s awareness of the device should factor into the Katz/Kyllo analysis.

What is more, “availability” and “social norms” interact in an unexpected way when common components are repurposed to an uncommon end. For example, well-known (fictional) government agent MacGyver could use his Swiss army knife to cobble together a working proof-of-concept from whatever ordinary items he had at hand, and use it to save the day. His end device was not “available” by itself, even if its components were common. Plus, the audience was supposed to find his creation a remarkable accomplishment. That is, in reality, maybe people could assemble a sleeping bag, some vodka, and an oxygen tank into a bomb in order to escape a plane buried in an avalanche, but what people (most of whom are not genius scientists) probably would actually do in that situation is get comfortable in the sleeping bag, alternate between hits

324 Id. at 440; see also id. at 438 (“What unrelated private persons actually do is a much more limited universe than what they are theoretically able or permitted to do.”).

325 Id. at 445 (footnote omitted).

326 Id.


329 Id.


of vodka and pure, sweet oxygen, and quietly resign themselves to the looming inevitability of death.

To cut to the chase: under Professor Henderson’s norms-based approach, if MacGyver had ever grabbed some common household items and built a side-channel device to spy on a suspected bad guy, a court applying the *Kyllo* test would not consider the resulting contraption to be “in general public use” no matter how quotidian its components.334

This Article therefore proposes the following factors for courts to consider in determining whether a sense-enhancing device is “in general public use,” building upon the LaFleur and Henderson models: How much does it cost? How easy is it to get (i.e., can people buy it at Radio Shack, or from Amazon or eBay)? Is it legal to own and use? Is it common among the general public? If not, is it common within an established niche market or community, and how aware is the general public of that niche use? How much assembly is required to use the device, and how common are its components? These considerations should be evaluated in totality to determine whether the technology at issue is “in general public use,” with the fundamental factors of cost, availability, and legality being accorded the most weight.

2. *Is Side-Channel Attack Equipment “in General Public Use”?*

Finally, let us apply the “general public use” factors suggested above to side-channel attack equipment.

For starters, *Kyllo*, with its thermal-imaging devices (which measure side-channel information about a home’s relative warmth), would probably come out differently today. Writing in 2002, LaFleur predicted that thermal-imaging devices like the one in *Kyllo* would one day be found on the shelves at Radio Shack (unless restricted by law), and that thermal-imaging technology “might be found not to be a search” if the same fact pattern in *Kyllo* were decided now.335 Fully seven years ago, Professor Kerr opined that this state of affairs had indeed come to pass.336

A more recent real-world case is also instructive, though it did not

---

334 Outside the context of side-channel attacks, an ingenious “one-off” MacGyver device might be deemed “in general public use” if it is a stand-in for an existing device that is undeniably in general public use, such as a defibrillator. See Greenspan, *supra* note 332 (describing the episode “The Enemy Within”).

335 LaFleur, *supra* note 281, at 945 (emphasis added).

actually apply *Kyllo*. In *United States v. Stanley*, law enforcement agents used a software/hardware equipment combination to track down a suspected child pornography offender.337 Called the “MoocherHunter,” the software/equipment combination “is a mobile tracking software tool that can be downloaded for free from the manufacturer’s website and used by anyone with a laptop computer and a directional antenna” to track down the wireless card of a computer that is “mooching” off a wifi signal.338 The government did not contend that the “MoocherHunter” was technology “in general public use” under *Kyllo.*339

The Third Circuit did not question that position, because it declined to apply the *Kyllo* “general public use” test.340 If we do so, then, applying the “in general public use” factors outlined above, cost favors an “in general public use” finding. The software was free, and a directional antenna can be ordered online for around $50.341 Likewise availability: the software was available for download, laptops are everywhere, and directional antennas are common enough. However, the fact that MoocherHunter was developed for law enforcement use342 cuts the other way, apparently dispositively. The general public is probably not aware of this niche software tool for the law enforcement community. Thus, while a laptop

---

337 753 F.3d 114, 115–17 (3d Cir. 2014).
338 Id. at 116. The court used the term “MoocherHunter” to refer collectively to the software and the equipment using it. Id. at 116 n.5. While wifi signal emissions can be considered side-channel information, the government’s use of MoocherHunter was not a side-channel attack *per se*.
339 Id. at 119. Before using the MoocherHunter, state and federal government agents discussed whether to obtain a warrant, and decided not to, both out of practical considerations and the distinctions they drew between the MoocherHunter and *Kyllo.* Id. at 117.
340 Id. at 119–20. Instead, the court concluded that by intentionally sharing contraband child pornography online using his neighbor’s wifi connection, “Stanley deliberately ventured beyond the privacy protections of the home, and thus, beyond the safe harbor provided by *Kyllo.*” Id. (citation omitted). This has led *Stanley* to be criticized as wrongly decided. See Andersen, supra note 298, at 2–3. Professor Kerr, by contrast, considers *Stanley* to be correctly decided under the third-party doctrine.
341 Id. at 119. E.g., *Yagi WiFi Antenna 2.4GHz Outdoor Directional 14d*, SIMPLEWiFI, http://www.simplewifi.com/yagi-wifi-antenna-2-4ghz-outdoor-directional-14d.html (last visited Apr. 10, 2017) (selling for $54.00). [https://perma.cc/HR4L-U2FA] The *Stanley* opinion does not specify what make and model of directional antenna was used. However, in a MoocherHunter demonstrational video, the software’s developers use an antenna that appears highly similar to the $54 white Yagi antenna. *Id.* See The *OSWA-Assistant(tm)*, THINKSECURE, http://securitystarthere.org/page-training-oswa-assistant.htm#moocherhunter [https://perma.cc/3NPB-BTT7] (embedded video displays directional antenna starting at approximately 13:40 minutes) (last visited Apr. 10, 2017).
and a directional antenna are affordable, available, and legal, once they were combined with obscure software for police use, the government in *Stanley* did not try to argue that the overall MoocherHunter hardware/software combination was in general public use.

Next, reviewing the key-extraction techniques discussed in Section I above, some would not fare well under a *Kyllo* analysis informed by *Stanley* and the “in general public use” factors suggested above. This is due to cost. The Genkin team’s through-the-wall EM key-extraction attack used an antenna that costs 500 euro—expensive enough to put that attack in the “not in general public use” category. Likewise, the “portable” microphone set-up the team used to enhance the range of their RSA key-extraction attack was lab-grade equipment too expensive and specialized to be “in general public use.” Those attacks require a warrant under *Kyllo*.

But otherwise, the Genkin team made it a point to use cheap hardware components that can be ordered off eBay or scavenged from equipment already in one’s possession. The expensive “portable” set-up for the RSA key-extraction attack can be substituted by a variation that uses just a mobile phone (though the attack then works only up to 30 centimeters).

And in the case of the “pita bread” attack, the team developed an alternative to the pita bread set-up that requires only a regular household radio, plus an audio recorder to record the signal output.

The mobile-phone and consumer-radio set-ups check off the crucial cost, availability, and legality boxes—they are common among the general public—and they minimize the “some assembly required” factor. A mobile phone, “innocuously place[d] . . . on the desk next to the target

---


345 *ECDH Key Extraction*, supra note 42, at 1, 15–16; *STEALING KEYS FROM PCS*, supra note 40, at 4 (attack “us[ed] simple and readily available equipment” or, in the alternative, “a common, consumer-grade radio,” again “avoid[ing] the expensive equipment used in prior attacks”).

346 *RSA Key Extraction*, supra note 41, at 10–11, 27.

347 *STEALING KEYS FROM PCS*, supra note 40, at 22–23. The pita bread set-up itself did not require anything expensive or hard to obtain; it used a software-defined radio (SDR) dongle, *id.* at 14, 21, which is arguably cheap and available enough to be, taken alone, “in general public use.” See Woodward, supra note 23 (noting that SDRs cost less than £30).

348 All of the equipment the team used in the various attacks is presumably legal to own, otherwise the researchers might have thought twice about talking about it in a series of published papers.
laptop” in order to secretly measure its EM emissions would likely qualify under *Kyllo* as a “sense-enhancing” device that is “in general public use.” Therefore, a court might rule that police need not get a warrant to conduct that particular key-extraction attack in that particular manner. A court might well reach the same conclusion as to the attack that requires only a consumer-grade radio and an audio recorder.

The Genkin team’s research demonstrates that side-channel attack equipment can potentially “pass” the *Kyllo* “general public use” test if law enforcement repurposes common items, such as a cell phone or radio, to new, surveillance-oriented purposes—without even having to “MacGyver” a bunch of parts together.

For perspective, repurposing common household items on the cheap to do a side-channel attack is a thirty-year-old strategy. Wim van Eck’s TEMPEST-style attack against a monitor (now popularly named after him) cost him $15 in equipment and a regular TV set in 1985. A side-channel attack involving “van Eck phreaking” of a target’s computer monitor almost certainly would not require a warrant under the *Kyllo* “general public use” test in 2017. Indeed, LaFleur, writing back in 2002, believed that the *Kyllo* ruling would likely extend to a TEMPEST-style attack using a device that “is completely passive and detects the modulated electromagnetic emissions from the [computer’s] keyboard or display” from a vantage point outside the building.

It may seem like a surprising outcome that some side-channel attacks do not require a warrant. In practice, a court might prove reluctant to allow “technology to shrink the realm of guaranteed privacy” in the electronic devices that hold so many details of our lives. Few laypeople have probably heard of side-channel cryptanalysis, so allowing the warrantless use of an “in general public use” cell phone or household radio, repurposed into “sense-enhancing technology” to extract private encryption keys from a laptop, may be a bridge too far. Applying Professor Henderson’s “social norms” factor, people could repurpose a phone or radio into surveillance devices, but that is not what people actually do. The court might be tempted to reject the application of the *Kyllo* test, as the Third Circuit did in *Stanley*, and resort to the classic *Katz* inquiry. If the court “ask[s] whether people reasonably expect” that their computers’ electromagnetic

---

349 *RSA Key Extraction*, supra note 41, at 5–6.
350 *Stealing Keys from PCS*, supra note 40, at 22–23.
351 van Eck, supra note 17, at 270; see also Christopher J. Seline, *Eavesdropping on the Compromising Emanations of Electronic Equipment: The Laws of England and the United States*, 23 Case W. Res. J. Int’l L. 359, 359 (1991) (putting the price point for “seeing what someone is typing on their computer screen from several hundred yards away” at under $200 in “easily-available parts” in an article published ten years before the *Kyllo* decision).
352 LaFleur, supra note 281, at 948.
emissions “will be recorded” and analyzed “in a manner that enables the government to ascertain, more or less at will,” their private keys (and thus the plaintext of their private information), then the government’s warrantless use of a side-channel key-recovery attack might be held not to pass constitutional muster.

Professor Henderson’s “social norms” factor was not expressly included in the Supreme Court’s formulation of the Kyllo rule, but it may be required to reconcile Kyllo with Katz’s “reasonable expectation” yardstick in order to avoid a result many would consider absurd. A straightforward inquiry into whether a device is “in general public use” that does not account for a non-standard use of that technology may be too “mechanical [an] interpretation of the Fourth Amendment.” Thus, to the Kyllo “general public use” factors listed above, it may be necessary to add yet another: If the device itself is in general public use, has it been modified or otherwise used in a non-standard manner? That is, is the use not a “general public use”? Adding that element would tilt the Kyllo factors more decisively toward the conclusion that, for each of the clever side-channel attack equipment set-ups discussed above, the device is not in general public use and thus requires a warrant when employed by police.

F. The Katz/Kyllo Framework Cannot Adequately Protect Privacy Against Advances in Law Enforcement Technology

Kyllo attempted to announce a rule the Court anticipated could be applied flexibly to unknown future technologies without compromising traditional privacy interests. In practice, however, this rule guaranteed that evolving technologies would gradually eat away at privacy over time.

The very possibility that a court might hold that the mobile-phone and household-radio attacks (or a van Eck phreaking attack) do not need a warrant illustrates a shortcoming of the Kyllo test and of the Katz approach more generally. Kyllo’s “not in general public use” rule was the Court’s strategy for preserving longstanding expectations of privacy against the encroachment of modern technology. The Court chose not to draw a line at a particular level of technological sophistication or complexity (which was wise), but rather, to focus on the technology’s obscurity.

This makes intuitive sense under the Katz “reasonable expectation of privacy” test, yet at the same time it highlights a notorious difficulty of that test. What is considered objectively reasonable changes over time, as societal norms shift and technology progresses. Under Katz and Kyllo,

---

355 Kyllo, 533 U.S. at 35.
356 See Jones, 565 U.S. at 427 (Alito, J., concurring) (stating that the Katz test assumes people have “a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in
the bar for government action to comport with the Fourth Amendment is gradually lowered, as once-wondrous inventions become humdrum—and people resign themselves to the lessening of their privacy.

This approach does not square with encryption’s vital role in the twenty-first century. Millions of Americans now use encryption to protect the security and privacy of their electronic devices and data from snoops, hackers, thieves, and other criminals—giving those bad actors an incentive to devise new methods for undermining cryptographic protections. Under the Katz/Kyllo framework, the proliferation of devices for bad actors to sidestep encryption would perversely result in the relaxation of the warrant requirement for seizures by the state. That is, the nefarious ingenuity of criminals would lessen the constitutional constraints placed on the very authorities charged with protecting us from them.

Absent a better rule for limiting technology’s incursions on privacy, the eventual impact could be dire. “All human activity is susceptible to observation in the form of energy reflection or emanation that is readily captured and converted to ‘data.’” If the courts permit side-channel data about us to be “pervasively captured, stored, and integrated with other data” by police without so much as a warrant, “individual privacy becomes a physical impossibility.” That is not the outcome the Kyllo Court intended—quite the contrary—but that is how it may play out, as long as Kyllo remains good law and the courts must continue to apply Katz to novel forms of non-trespassory surveillance.

CONCLUSION

Once side-channel attacks make the eventual jump from military and intelligence to law enforcement use, judicial challenges to their constitutionality will soon follow. This Article illustrates the shortcomings of the present legal framework (such as it is) for seizure of encryption keys

357 See id. at 415 (Sotomayor, J., concurring) (“the same technological advances that have made possible non-trespassory surveillance techniques will also affect the Katz test by shaping the evolution of societal privacy expectations”) (citing id. at 427 (Alito, J., concurring)).

358 See id. at 427 (Alito, J., concurring) (“[E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.”) (footnote omitted).

359 LaFleur, supra note 281, at 948.

360 Id.


362 Jones, 565 U.S. at 411 (“Situation involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis.”).
by means of a side-channel attack.

Side-channel attacks that law enforcement conducts against electronic devices located in a home or office are analyzed under the Kyllo framework. Because the Fourth Amendment strongly protects those spaces, obtaining side-channel information from devices inside them generally requires a warrant. However, Kyllo’s “general public use” rule opens up an exception. In time, that exception will permit the warrantless seizure of side-channel information from an otherwise constitutionally-protected space if the devices to do so become common enough. That rule is not a principled way to make a decision about the privacy protections for an encryption key, and the decision should not be left up to the courts.

For side-channel attacks conducted in public spaces, Jones dictates that the Katz “reasonable expectation of privacy” analysis applies. There is generally a reasonable expectation of privacy in our electronic devices and the information (including encryption keys) they contain. Therefore, the Fourth Amendment will typically require a warrant for the seizure of encryption keys via side-channel key-extraction attacks in public, as it does for the home. Similarly, however, that standard will be undermined if the Kyllo rule extends beyond the home context to non-trespassory surveillance of electronic devices in public spaces.

In short, when it comes to cryptographic side-channel attacks, current Fourth Amendment jurisprudence is ill-equipped to safeguard Americans’ privacy in the long term. What reform is most appropriate is beyond the scope of this Article. That said, anticipating the advent of cryptographic side-channel attacks by law enforcement presents a rare opportunity for us to shape the law now, rather than reacting to technological change after the fact. We would be well-advised not to waste that chance.