NOTE

"YOU'VE TAKEN ALL YOU CAN BEAR"[1]: REPLACING THE RICKETY FRAMEWORK FOR LAW ENFORCEMENT ACCESS TO PRIVATE COMMUNICATIONS

JOHN S. CONNOLLY*

In 1986, mail was sent through the U.S. Postal Service, a search engine was called a library, "tweets" were the sounds made by birds in the trees, and "clouds" were found only in the sky.[2]

—Congressman Bob Goodlatte (R-Va.)

Abstract: One of the most surprising episodes of the first hundred days of the Trump Presidency was President Trump's tweet stating "that Obama had [his] 'wires tapped' in Trump Tower just before the victory."[3] *Of the many questions this accusation raised, one of the most pointed was whether then-candidate Trump or his organization were under criminal investigation such that a criminal wiretap could have been authorized.*[4] *This question was natural because*

---

[1] A line from Cyndi Lauper's 1986 hit "True Colors," which topped the charts the last time a major overhaul of domestic communications surveillance in the United States was enacted. *See* CYNDI LAUPER, *True Colors, on* TRUE COLORS (Portrait Records 1986); *see also The Hot 100 - 1986 Archive*, BILLBOARD CHARTS ARCHIVE, http://www.billboard.com/archive/charts/1986/hot-100 [https://perma.cc/P55V-AFEY] (listing "True Colors" as the top song for the week ending October 25, 1986).

* Associate, Williams & Connolly LLP; J.D., Harvard Law School, 2016; A.B., Bowdoin College, 2011. Thanks to professors Susan Crawford, Andrew Crespo, and Alex Whiting, whose classes inspired and contributed to this Note. Many thanks also to the members of the *Harvard Journal on Legislation* for their help, particularly Paul Kominers, George Maliha, Melissa Greenberg, Coco Xiao, Chanslor Gallenstein, Joshua Holtzman, Madison Reddick, Samantha Fry, Sadie Hillier, Louis Murray, Madeline Salinas, and Tessa Vellek. Any errors are the author's and not theirs.

[2] Press Release, U.S. House Comm. on the Judiciary, Goodlatte: Email Privacy Act Embodies the Principles of the 4th Amendment (Apr. 27, 2016), https://judiciary.house.gov/press-release/goodlatte-email-privacy-act-embodies-principles-4th-amendment/ [https://perma.cc/YRF6-UG3K].

[3] *See* Darlene Superville & Catherine Lucey, *Moments That Matter in Trump's First 100 Days in Office*, ASSOCIATED PRESS, Apr. 27, 2017 (quoting Donald J. Trump (@realdonaldtrump), TWITTER (Mar. 4, 2017, 6:35 AM), https://twitter.com/realdonaldtrump/status/837989835818287106 [https://perma.cc/Q8VW-RA6X]), https://elections.ap.org/content/moments-matter-trumps-first-100-days-office [https://perma.cc/FWG3-KGNU].

[4] *See* Benjamin Wittes, *Ten Questions for President Trump*, LAWFARE (Mar. 4, 2017, 11:46 AM), https://www.lawfareblog.com/ten-questions-president-trump [https://perma.cc/DC2D-ZF6Q]; *see also* Charlie Savage, *What Can Be Gleaned from the President's Allegations on Twitter of Wiretapping*, N.Y. TIMES, Mar. 6, 2017, at A13, https://www.nytimes.com/2017/03/05/us/politics/trump-phone-tapping-surveillance-issues.html [https://perma.cc/P3BH-5NB6] ("If it was a criminal wiretap, it would mean that the Justice Department had gathered sufficient evidence to convince a federal judge that someone using the phone number or email address probably committed a serious crime.").

federal law sets a high bar for government officials seeking real-time access to a person's phone calls or emails.[5] *But if President Trump had instead accused President Obama of accessing all his emails from the previous few years, the accusation would have been more plausible legally (if not factually) because law enforcement can theoretically obtain emails older than 180 days by issuing a simple subpoena.*[6] *Does this difference make any sense?*

This Note examines the current framework for law enforcement access to private communications and proposes concrete ideas to make that framework coherent.[7] *Specifically, it advocates adopting a new system for deciding what authorization law enforcement must receive to access different types of communications. This system would be based on the scope of the access and the sensitivity of the material sought.*

Table of Contents

[5] As it turns out, some of then-candidate Trump's phone calls may incidentally have been intercepted due to surveillance of his campaign chairman, Paul Manafort, under the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1888 (2012). *See* Matt Ford, *Five Questions About the Manafort Investigation*, Atlantic (Sept. 19, 2017), https://www.theatlantic.com/politics/archive/2017/09/five-questions-about-the-manafort-investigation/540270/ [https://perma.cc/6A2U-AUVS]. FISA and the surveillance conducted pursuant to it are beyond the scope of this Note.

[6] *See* 18 U.S.C. § 2703 (2012).

[7] There is yet another framework for matters involving national security or foreign actors. This Note confines itself to more run-of-the-mill domestic criminal matters.

I. Introduction

The framework controlling law enforcement access to communications such as email, text messages, call records, and related data like real-time locations is in disarray.[8] This access involves at least six statutes or rules[9] and nine types of legal process, the legal instruments used by law enforcement to gain access to communications (e.g., a warrant).[10] The process required for authorities to access a given communication depends primarily on the state of technology in 1986 when the last comprehensive law on the subject—the Electronic Communications Privacy Act ("ECPA")—was enacted.[11] The resulting distinctions are formalistic and counterintuitive. For example, a subpoena—a piece of paper many government agencies can issue with a signature—theoretically allows the government to access the text of all emails that have either been opened or stored online for more than 180 days.[12] But a search warrant is necessary to access unopened emails under the 180-day mark.[13] And real-time access to email as it arrives requires a "super-warrant," which must be signed by a federal district court judge, approved by a senior official with the Department of Justice, and is subject to many other restrictions.[14] These distinctions, based in large part on how email and telephone networks operated in the mid-1980s, have outlived their

---

[8] *See, e.g.*, Julie J. McMurry, *Privacy in the Information Age: The Need for Clarity in the ECPA*, 78 Wash. U. L.Q. 597, 601 (2000) (noting the "confusion" involved in interpreting the Electronic Communications Privacy Act ("ECPA"); Note, *A Thinly Veiled Request for Congressional Action on E-mail Privacy:* United States v. Councilman, 19 Harv. J.L. & Tech. 211, 230 (2005) (referring to the jurisprudence surrounding the Electronic Communications Privacy Act (ECPA) as "a muddled morass").

[9] *See* 18 U.S.C. §§ 2518, 2703, 3117, 3122, 3123 (2012); Fed. R. Crim. P. 41.

[10] *See* Title III super-warrants, 18 U.S.C. § 2518, *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294, 305 (E.D.N.Y. 2005), search warrants, Fed. R. Crim. P. 41; Electronic Communications Privacy Act ("ECPA") warrants, 18 U.S.C. § 2703(g), § 2703(d) orders, 18 U.S.C. § 2703(d), pen register/trap and trace orders, 18 U.S.C. § 3123 (2012), trial subpoenas, Fed. R. Crim. P. 17, grand jury subpoenas, Fed. R. Crim. P. 17; administrative subpoenas, 18 U.S.C. § 3486 (2012).

[11] *See* ECPA, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.); Declan McCullagh, *Google, Facebook go retro in push to update 1986 privacy law*, CNET (Oct. 21, 2011), http://www.cnet.com/news/google-facebook-go-retro-in-push-to-update-1986-privacy-law/ [https://perma.cc/RE6N-CTPV].

[12] *See* 18 U.S.C. § 2703. While the law still authorizes such searches with only a subpoena, most tech providers themselves have required a search warrant since the Sixth Circuit case *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), which is discussed below. *See* Allison Grande, *Microsoft Says Warrantless User Content Demands Won't Fly*, Law360 (Mar. 21, 2013), http://www.law360.com/articles/426171/microsoft-says-warrantless-user-content-demands-won-t-fly [https://perma.cc/843Z-PXRD].

[13] *See* 18 U.S.C. § 2703.

[14] *See* 18 U.S.C. § 2518. These warrants, from the original Wiretap Act, are sometimes called "super-warrants" because of the heightened requirements over traditional search warrants. *See* Susan Freiwald, *Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 13 n.22, 25 (2004).

usefulness. The chart in Appendix A—from a manual for federal prosecutors—demonstrates the chaotic state of the current system.[15]

These problems are not solely academic. They implicate fundamental questions about privacy and due process.[16] They also impose enormous compliance costs on both business[17] and government.[18] They confound the judiciary.[19] Even law enforcement agrees that aspects of the current system make little sense.[20] Change is long overdue, but if Congress does not address ECPA's problems comprehensively, any changes it puts in place will soon be as outdated as the current law. Moreover, Congressional indecision may force the Supreme Court to act. This Term, for example, the Court is considering in *Carpenter v. United States*[21] whether the warrantless seizure and search of historical cell phone location records that reveal a phone's movement over a period of several months violate the Fourth Amendment. Congress is far better equipped to fix ECPA than the Court; it must do so.[22]

Proposals to reform ECPA and its technology-based regime are often incremental: they suggest extending current protections to cover new interception technology or heightening the protections already in place.[23] Indeed,

---

[15] *See infra* Appendix A. While this chart has yet to be updated with recent court decisions and guidance from the Department of Justice, the framework is still just as fragmented.

[16] *See Statement on Protecting Internet Privacy and Due Process*, INTERNET INFRASTRUCTURE COAL. (Nov. 29, 2012), http://www.i2coalition.com/statement-on-protecting-internet-privacy-and-due-process/ [https://perma.cc/6SUX-HTA2].

[17] Sprint, for example, developed a new web portal dedicated to law enforcement just to keep up with demand. *See* Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, WIRED (Dec. 1, 2009), http://www.wired.com/2009/12/gps-data/ [https://perma.cc/UD8E-T5BV]; *see also* Anthony L. Hall & Adam G. Lang, *Beware Accessing Employees' Personal E-mail May Result in Severe Penalties*, 15 NEV. EMP. L. LETTER 1 (2009).

[18] *See* Anne Flaherty, *What the Government Pays to Snoop on You*, USA TODAY (July 10, 2013, 8:30 AM), http://www.usatoday.com/story/money/business/2013/07/10/what-government-pays-to-snoop-on-you/2504819/ [https://perma.cc/9UTD-TJ28].

[19] *See* Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J., Sept. 22, 2011, at A1.

[20] *See Reforming the Electronic Communications Privacy Act*, *Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 4 (2015) (statement of Elana Tyrangiel, Principal Deputy Assistant Att'y Gen., United States Department of Justice), https://www.judiciary.senate.gov/imo/media/doc/09-16-15%20Tyrangiel%20Testimony.pdf [https://perma.cc/BM8L-HPR3] (agreeing, *inter alia*, "that there is no principled basis to treat email less than 180 days old differently than email more than 180 days old").

[21] Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017) (mem.).

[22] *See* Jennifer Daskal, *Where Is Congress? The Supreme Court's Cert in Microsoft Ireland Case Should Spur Lawmakers to Act*, JUST SECURITY (Oct. 18, 2017, 1:42 PM), https://www.justsecurity.org/46075/congress-supreme-courts-cert-microsoft-ireland-case-spur-congress-act/ (arguing that another ECPA case to be decided this Term "highlights the need for Congress to step in, update the underlying statute with the nuance that it deserves, and thereby moot the case").

[23] *See, e.g.*, Email Privacy Act, H.R. 1852, 113th Cong. (2013) (modifying ECPA only as to the contents of communications by requiring a warrant for them); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 166–69 (2013) (advocating that the Pri-

legislation that passed the House of Representatives in February 2017 modifies ECPA by requiring a warrant for all access to email and files stored on the cloud.[24] While a positive change, this bill is a bandage for something that requires major surgery.

On the other side of the spectrum, leading cyberlaw scholar Orin Kerr sketched the outlines of an ideal "Next Generation Communications Privacy Act"[25] that would, among other things, enact a uniform standard for access to content[26] and require that law enforcement requests for noncontent data[27]—like the phone numbers a person has dialed—be narrow in scope.[28] This broad proposal envisions a completely new system for domestic communications access by law enforcement, although it is more a thought experiment than an outline for legislation.

This Note charts a middle course. Its proposals are broader than the ECPA updates currently being pursued in Congress but specific enough that they could be enacted without completely dismantling the current domestic communications access framework. Chiefly, it advocates an overhaul of that framework that would make an expanded Wiretap Act the basis of our communications access regime. This overhaul would assign different legal process requirements to law enforcement communications access based on the scope of that access and the sensitivity of the accessed material. That is, the approval process required for law enforcement to access a particular message should not be different for emails and phone calls, but that process should be different when accessing a single phone's call history versus the call history of the thousand phones in a particular area. Additionally, this Note proposes making this access scheme all-encompassing so law enforcement's access to communications would operate within a consistent framework, regardless of technology, and would not require further legislation.

At first blush, these changes may seem no less flawed than the system put in place by ECPA in 1986. There, the length of time a communication

---

vacy and Civil Liberties Oversight Board regularly study law enforcement surveillance and report thereon to Congress).

[24] *See* Email Privacy Act, H.R. 387, 115th Cong. (2017) (as passed by the House on February 6, 2017).

[25] *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 375–78 (2014).

[26] *See id.* at 411–12.

[27] Noncontent data is often referred to as metadata, but the concept of content versus noncontent data has a long history in surveillance law. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979) (distinguishing recording devices from "pen registers," which record the numbers a phone dials, by emphasizing that "pen registers do not acquire the *contents* of communications"). Courts have struggled with the line between content and noncontent data, and the distinction arguably no longer makes sense given modern communications networks. *See* Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 2–3 (2016). This Note retains both the term and concept of noncontent data in keeping with this Note's proposal to overhaul the existing communications surveillance framework while maintaining the components of that framework that still make sense.

[28] *See* Kerr, *The Next Generation Communications Privacy Act*, *supra* note 25, at 412–14.

was stored and its means of storage were meant to be technology-neutral ways of limiting access. As technology evolved, however, these criteria became less and less relevant. Time and storage seem to have been intended as proxies for what really matters—privacy. Leaving an email stored on somebody else's server for 180 days was seen as an indication that the recipient did not care to protect the contents of that message.[29] With the rise of low-cost storage and the cloud, this assumption no longer holds. This Note's scheme is superior because it does away with proxies and deals with the actual concern—privacy. The two factors that judges must balance under this Note's proposal—sensitivity and scope of access—are the actual concerns that citizens have expressed with government surveillance going back to *Olmstead v. United States*[30] in 1928. These concerns will not become outmoded as technology develops, so they are the best way to ensure law enforcement needs are balanced against privacy interests.

II. The Communications Surveillance Landscape

A. *History of Communications Surveillance Law in the United States*[31]

Communications interception in the United States began shortly after the introduction of the telegraph in 1844, and wiretaps were commonly used during the Civil War.[32] The Supreme Court took up wiretapping for the first time in *Olmstead*.[33] Relying on the lack of physical intrusion into the defendant's premises and construing the sense of hearing not to constitute a search or seizure, the majority held that a wiretap did not violate the Fourth Amendment.[34]

---

[29] The common understanding of the motivation behind the 180-day limit for heightened protection of email is that in 1986 a user who left an email unopened on another's system for 180 days was viewed to have abandoned it. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1234 (2004) ("The apparent thinking behind the lower thresholds for government access of both permanently stored files and unretrieved files stored for more than 180 days is that the lower thresholds track Supreme Court precedents interpreting the Fourth Amendment. . . . [T]he strange '180 day rule' . . . may reflect the Fourth Amendment abandonment doctrine at work. Individuals lose the Fourth Amendment protection in property if they abandon the property, and the [Stored Communications Act's] drafters may have figured that unretrieved files not accessed after 180 days have been abandoned." (footnote omitted)).

[30] 277 U.S. 438, 471, 474–76 (1928) (Brandeis, J., dissenting). Justice Brandeis' dissent is foundational in the field of privacy law.

[31] This summary is in no way intended to be comprehensive. For a more extensive history of the Fourth Amendment's application to wiretaps, see generally Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004).

[32] *See* Daniel J. Solove et al., Privacy, Information, and Technology 64 (2006).

[33] 277 U.S. at 438.

[34] *See id.* at 466.

Congress spoke next by passing the Communications Act of 1934, which included a provision restricting interception and divulgence of communications by anyone not authorized by the sender.[35] The Department of Justice, however, viewed its own interceptions as not falling under this prohibition as long as it only divulged information to public officials.[36] In 1967, the Supreme Court issued a pair of decisions that changed the landscape for law enforcement use of wiretaps and electronic surveillance: *Berger v. New York*[37] and *Katz v. United States*.[38] In *Berger*, the Court examined and struck down the New York wiretap statute because it authorized law enforcement to wiretap suspects without providing sufficient Fourth Amendment safeguards.[39] In *Katz*, the Court dealt with an electronic bug rather than a wiretap.[40] Here, the Court overturned *Olmstead*,[41] and in a famous concurrence, Justice Harlan articulated what has become the dominant "reasonable expectation of privacy" test.[42] The modern formulation of this test is that when a person has a reasonable expectation of privacy, police actions violating that expectation are unconstitutional without a warrant unless some exception applies.[43]

Against the backdrop of these Supreme Court decisions, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, Title III of which concerned "Wiretapping and Electronic Surveillance."[44] This title is known as both "Title III" and "The Wiretap Act."[45] Broadly, the Act outlawed the "intercept[ion of] any wire or oral communication" except as specifically authorized.[46] For federal law enforcement, that authorization requires obtaining what have become known as "super-warrant[s]."[47] These warrants are much more difficult to obtain than traditional search warrants

---

[35] *See* Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064.

[36] *See* Herbert Brownwell, Jr., *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195, 197 (1954).

[37] 388 U.S. 41 (1967).

[38] 389 U.S. 347 (1967).

[39] "The Berger opinion tells us that to be constitutional, a wiretapping law must require: a) that 'a neutral and detached authority' evaluate whether probable cause exists before wiretapping occurs; b) that the application for the court order to explain '[w]hat specific crime has been or is being committed,' 'the place to be searched,' and 'the persons or things to be seized'; c) that the order authorizing the wiretapping 'places a termination date' on the surveillance; d) that there is 'notice as [with] conventional warrants,' or 'some showing of special facts' to excuse notice; and e) 'a return on the warrant.'" Kerr, *The Fourth Amendment and New Technologies*, *supra* note 31, at 848 (footnotes omitted) (quoting *Berger*, 388 U.S. at 54–60).

[40] *See id*. at 849 (citing *Katz*, 389 U.S. at 348).

[41] *Katz*, 389 U.S. at 353.

[42] *Id*. at 360 (Harlan, J., concurring).

[43] *See* Kerr, *The Fourth Amendment and New Technologies*, *supra* note 31, at 808.

[44] Pub. L. No. 90-351, 82 Stat. 197 (1968).

[45] *See* Kerr, *The Next Generation Communications Privacy Act*, *supra* note 25, at 379 n.22.

[46] Omnibus Crime Control and Safe Streets Act, § 2511(1)(a).

[47] *See* Freiwald, *supra* note 14, at 25.

and are limited in both time and scope.[48] The Wiretap Act continues to govern telephone wiretaps and the placement of listening devices today, and it provides the framework within which subsequent restrictions—including those suggested by this Note—fit.[49]

The Supreme Court contributed the next piece to the communications interception puzzle with its decisions in *United States v. Miller*[50] and *Smith v. Maryland*.[51] In *Miller*, the Court ruled that the Fourth Amendment did not protect information revealed to a third party from being turned over to the government in response to a subpoena.[52] In *Smith*, the Court noted that "a person has no legitimate expectation of privacy in the information he voluntarily turns over to third parties" and held that law enforcement could intercept phone numbers dialed using a "pen register" device without judicial oversight because this interception was not a search under the Fourth Amendment.[53] Together, these cases resulted in what is known as the third-party doctrine: the government can, without obtaining a warrant,[54] access information given voluntarily to third parties.[55]

Seven years later, Congress enacted the Electronic Communications Privacy Act of 1986.[56] ECPA was the last major piece of domestic law enforcement communications access legislation, and its three titles provide most of the modern law in this area. Title I expanded the Wiretap Act to include contemporaneous interception of data.[57] Title II—known as the Stored Communications Act—enacted the most sweeping changes.[58] It pro-

---

[48] *See id.*

[49] *See* Kerr, *The Fourth Amendment and New Technologies*, *supra* note 31, at 850.

[50] 425 U.S. 435 (1976).

[51] 442 U.S. 735 (1979).

[52] *See Miller*, 425 U.S. at 442–43.

[53] *Smith*, 442 U.S. at 743–46.

[54] Some courts recently have resisted the notion that law enforcement can access an unlimited amount of information about a suspect without a warrant—even when each individual piece of information has been revealed to a third-party or the public at large—because the information aggregated infringes on the suspect's reasonable expectation of privacy. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("As with the 'mosaic theory' often invoked by the Government in cases involving national security information, [w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene." (internal quotation marks omitted)). *See generally* Joshua Vittor, *What Would a Martian Think of Cell Phones? The Third-Party Doctrine and Technological Extensions of the Human Self*, 10 HARV. L. & POL'Y REV. 255 (2016) (surveying courts' recognition of the increasing tension between the third-party doctrine and the pervasiveness of modern technology).

[55] John Villasenor, *What You Need to Know about the Third-Party Doctrine*, THE ATLANTIC (Dec. 30, 2013), http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ [http://perma.cc/UHM4-BBBB].

[56] Pub. L. No, 99-508, 100 Stat. 1848 (1986).

[57] *See id.* tit. I; Kerr, *The Next Generation Communications Privacy Act*, *supra* note 25, at 382.

[58] *See* tit. II, 100 Stat. at 1860; Kerr, *The Next Generation Communications Privacy Act*, *supra* note 25, at 383.

vided some protections to the customers of "electronic communication service[s] (ECS)" and "remote computing services (RCS)."[59] ECS providers are email services like Gmail or Yahoo! along with certain aspects of social media like a user's Facebook "wall."[60] RCS include any company that provides "computer storage or processing services by means of" the internet to the public.[61] Cloud storage providers like Dropbox clearly fit this definition.[62] Courts have also held that YouTube belongs in this category.[63] Finally, ECPA's Title III—the Pen Register Statute—responded to *Smith* by requiring a court order to place a pen register (tracking outgoing calls) or trap and trace device (tracking incoming calls) on a subscriber's telephone.[64]

Since its passage, ECPA has been modified several times. Congress enacted the most extensive changes in the 1994 Communications Assistance to Law Enforcement Act and 2001 PATRIOT Act, each of which altered the scope of various orders under ECPA.[65] More significantly, in 2010, the Sixth Circuit in *United States v. Warshak*[66] held unconstitutional the portion of ECPA that permitted warrantless access to emails.[67] Neither party sought Supreme Court review, so *Warshak* officially applies only in the Sixth Circuit. However, Google has begun demanding warrants to access customer email from law enforcement nationwide.[68]

B. Legal Process Required Under Current Law

This Part examines the types of legal processes and associated standards of review currently in use for communications access. For each type of legal process, it lays out what types of access the process covers, how common this access is, what law enforcement needs to do to obtain the process, what standard of review applies, and the involvement of the judiciary. Once again, the chart in Appendix A provides a summary of this information. The legal processes are laid out in order from most to least difficult to obtain.

---

[59] Kerr, *supra* note 25, *The Next Generation Communications Privacy Act*, at 383.

[60] Richard M. Thompson II, Cong. Research Serv., R43015, Cloud Computing: Constitutional and Statutory Privacy Protections 8–11 (2013).

[61] *See* § 201, 100 Stat. at 1848 (providing this definition).

[62] Eric P. Mandel, *A Hurdle to Obtaining Electronic Evidence*, Law360 (July 11, 2013, 11:45 AM), http://www.law360.com/articles/455225/a-hurdle-to-obtaining-electronic-evidence [https://perma.cc/E6TY-AK99].

[63] *See* Thompson, *supra* note 58, at 11–12.

[64] *See* Kerr, *supra* note 23, *The Next Generation Communications Privacy Act*, at 382–83.

[65] *Id.* at 385.

[66] 631 F.3d 266 (2010).

[67] *See id.* at 288 (holding that "to the extent that the SCA purports to permit the government to obtain . . . emails [stored by an ISP] warrantlessly, the SCA is unconstitutional").

[68] *See* David Kravets, *Google Tells Cops to Get Warrants for User E-mail, Cloud Data*, Wired (Jan. 23, 2013, 5:29 PM), https://www.wired.com/2013/01/google-says-get-a-warrant/ [http://perma.cc/R8G9-XBQN].

1. Super-warrants

These warrants authorize the interception of live telephone conversations, real-time access to sent and received emails, and surreptitious audio and video recording of private conversations. Federal judges granted 1,551 super-warrants in 2016 (the last year for which numbers are available).[69] More than that number were issued by state judges.[70] Eighteen of these warrants involved Google, representing less than 0.06% of the 27,850 (federal and state) government requests for data the company received in 2016.[71] As their name suggests, super-warrants are very difficult to obtain. Super-warrants are only available to investigate specific crimes and only once several requirements have been met: (1) authorization from a high-level Department of Justice[72] (or equivalent state) official, (2) justification of a wiretap's necessity in light of other possible investigative methods, (3) specific targets and locations of interceptions, (4) probable cause that the interception will uncover information about the targeted crime, and (5) details about the procedures law enforcement will use to minimize interception of irrelevant communications.[73] Unlike search and arrest warrants, many of which are issued by magistrate judges,[74] super-warrants must be issued by federal district court or court of appeals judges or any state judge similarly authorized.[75]

---

[69] *See* ADMIN. OFFICE OF THE U.S. COURTS, 2016 WIRETAP REPORT tbl.2 (2017), http://www.uscourts.gov/statistics-reports/wiretap-report-2016 [http://perma.cc/L54V-WE35].

[70] *See id.* (including only the numbers of jurisdictions that choose to issue reports).

[71] *Transparency Report*, GOOGLE, https://transparencyreport.google.com/user-data/overview?t=table&user_requests_report_period=series:requests,accounts,compliance;authority:US&lu=user_requests_report_period [https://perma.cc/8RUY-AX7F]. This report classifies super-warrants as wiretap order requests. *Id.*

[72] The act allows the Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal or National Security Divisions specifically designated by the Attorney General to authorize an application to a federal judge of the component jurisdiction for, and such judge may grant, an order authorizing or approving federal wiretaps. 18 U.S.C. § 2516 (2012 & Supp. IV 2017); *see* U.S DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL 9-7.100 (2012), https://www.justice.gov/usam/usam-9-7000-electronic-surveillance#9-7.100 [https://perma.cc/JTC4-8DLE].

[73] 18 U.S.C. §§ 2516–18 (2012 & Supp. IV 2017)).

[74] *See* Tim A. Baker, *The Expanding Role of Magistrate Judges in the Federal Courts*, 39 VAL. U. L. REV. 661, 680–81 (2005).

[75] *See* 18 U.S.C. § 2510(9) (2012); U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW 3 (2005).

2. Search Warrants and ECPA Warrants

There are two types of search warrants that apply to communications surveillance: traditional search warrants and so-called "ECPA warrants."[76] The warrants are substantially the same. Search warrants apply to the search and seizure of physical devices or records; ECPA warrants apply to the contents of protected electronic communications held by third-party providers. In addition to its division of ECS providers from RCS providers, ECPA also enacted a complex scheme of protections based on time. ECPA warrants—the highest level of process under ECPA—are the only way to access unopened emails stored for a period of less than 180 days. The government does not publish data on the number of warrants issued each year, but of the 27,850 (federal and state) government requests for data Google received in 2016, 8,264—a bit under 30%—were search or ECPA warrants.[77] These warrants must comply with Federal Rule of Criminal Procedure 41, so they must be based on probable cause.[78] Unlike traditional search warrants, ECPA warrants do not require the presence of an officer during service or execution.[79] A judge or magistrate reviews the affidavit supporting the warrant for probable cause.[80]

3. Court Orders

There are two types of court orders that apply to communications surveillance, and they are different enough to merit separate consideration. Moreover, law enforcement agencies often ask for a "hybrid" order consisting of both types of orders, which will also be discussed.

a. Section 2703(d) Orders

These orders—named after the section of ECPA from which they originate—are used to compel production of account activity logs from Internet Service Providers ("ISPs") that list what websites a subscriber visited, the "To" and "From" information for all emails in an email account, and his-

---

[76] *See* Josiah Dykstra & Damien Riehl, *Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing*, 19 RICH. J.L. & TECH. 1, 14 (2012) (explaining the differences between a "Rule 41 warrant" and an "ECPA warrant").

[77] *See* GOOGLE, *supra* note 71. In its data, Google does not differentiate between search and ECPA warrants, *see id.*, but given the type of content Google has access to, presumably all or nearly all are ECPA warrants.

[78] *See* 18 U.S.C. § 2703(a) (2012) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction."); Fed. R. Crim. P. 41(d).

[79] 18 U.S.C. § 2703(g) (2012).

[80] Fed. R. Crim. P. 41(d).

toric cell site location data providing the rough history of a person's movements.[81] Once again, the government does not disclose how often such orders are issued, but of the 27,850 requests Google received from governments in 2016, 2,362—over 8%—were "other court orders," a category that specifically includes § 2703(d) orders.[82] Applications for these orders must include "specific and articulable facts" showing that the information they seek is relevant to an ongoing criminal investigation. A judge or magistrate may issue the order, but they may not undertake an independent investigation of the facts alleged in the order request.

b. Pen Register / Trap and Trace Orders

These orders allow contemporaneous interception of noncontent information like outgoing and incoming phone numbers, outgoing and incoming websites, and the "To" and "From" fields of emails sent and received. In this way, they are the real-time counterpart of § 2703(d) orders. However, these orders cannot by themselves be used to obtain real-time cell phone location information.[83] The Department of Justice occasionally releases information about its agencies' pen register and trap and trace orders, and in 2013, these agencies obtained over 21,000 of each type of order.[84] In 2016, of the 27,850 requests Google received from governments, 518—a bit under 2%—were pen register orders.[85] Applications for a pen register and trap and trace order require a certification by law enforcement that the information likely to be obtained is relevant to an ongoing investigation. As with § 2703(d) orders, the federal judge or magistrate who approves these orders does not look beyond the applicant's certification of relevance.

c. Hybrid Orders

Because pen register orders specifically except real-time cell site location information, prosecutors began applying for such orders alongside § 2703(d) orders. Under the language of the statute, they argued these "hybrid" orders provided the authorization necessary for real-time cell site loca-

---

[81] *See* 18 U.S.C. § 2703(d).

[82] *See* GOOGLE, *supra* note 71. Although Google lists this category as "other court orders," the only "other" order it mentioned in the Transparency Report's FAQ is the § 2703(d) order. *See id.*

[83] *See The Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance*: *Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 6 (2013) [hereinafter "*ECPA Hearing*"] (statement of Mark Eckenwiler, Senior Counsel, Perkins Coie LLP).

[84] U.S. DEP'T OF JUSTICE, REPORT ON THE USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES BY THE LAW ENFORCEMENT AGENCIES/OFFICES OF THE DEPARTMENT OF JUSTICE FOR CALENDAR YEAR 2013, at 1 (2014), https://www.justice.gov/sites/default/files/criminal/legacy/2014/12/17/2013penreg-anlrpt.pdf [https://perma.cc/L59R-FF7W]. This report lists pen register and trap and trace requests separately, and the numbers are slightly different. *See id.* Because the vast majority of requests include both, the numbers have been averaged here.

[85] *See* GOOGLE, *supra* note 71.

tion information.[86] For the most part, district courts agreed with them,[87] but there has been increasing pushback since 2005,[88] and whether this procedure will be successful now depends on the district (and sometimes on the individual judge in each district).[89] If courts reject the hybrid order, they often require an ECPA warrant to access such information.[90]

4. Subpoenas

Subpoenas allow access to large amounts of content and noncontent data. There are three types of subpoenas relevant here—grand jury, trial, and administrative—each of which can be used to access the same information. On the content side, any opened email left on an email service's system and any unopened emails older than 180 days are retrievable by subpoena under ECPA. Although this is still technically the law in most of the United States, since the Sixth Circuit decided in *Warshak* that the contents of emails were protected by the Fourth Amendment, many email service providers have required law enforcement agencies nationwide to secure warrants in order to access these emails.[91] On the noncontent side, subpoenas allow access to a whole host of basic subscriber information including the name of the accountholder with an ISP or a cell phone provider, the IP address from which they established the account and from which they login, and the way they pay their monthly bills. Subpoenas have been and remain the most common way for law enforcement to access information, and of the 27,850 requests Google received from governments in 2016, 16,037—nearly 58%—were subpoenas.[92] The subpoena sets a low bar, as prosecutors and administrative agencies can effectively issue them at their own discretion.

---

[86] *See In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 n.6 (3d Cir. 2010) (collecting cases).

[87] *See id.*

[88] *See, e.g.*, *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) ("The government's hybrid theory, while undeniably creative, amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result. Viewing each statute in proper temporal perspective, there is simply no reason to believe that Congress intended to treat location monitoring of cell phones as an exceptional type of electronic surveillance. While Congressional enactments are sometimes difficult to decipher, employing such a three-rail bank shot to create a new category of electronic surveillance seems almost perverse. Had Congress truly intended such an outcome, there were surely more direct avenues far less likely to confound and mislead judicial inquiry.").

[89] *See ECPA Hearing*, *supra* note 83, at 7.

[90] *See id.*

[91] *See* Kravets, *supra* note 68; *Warshak*, 631 F.3d at 266.

[92] *See* GOOGLE, *supra* note 71.

III. The Wiretap Act as a Guide

A. What can we learn from the Wiretap Act and ECPA?

The Wiretap Act successfully has regulated law enforcement access to real-time communications for fifty years. ECPA, by contrast, was outdated within a few years of passage. Any new or updated law should look to the Wiretap Act's strengths while avoiding ECPA's weaknesses. As a nearly fifty-year-old law, the Wiretap Act holds up well. The 1968 Act still accomplishes its original purpose: telephone conversations may not be intercepted without use of a super-warrant. Courts readily have applied the law to new technologies such as cell phones, pagers, fax machines, and VoIP technology. Indeed, over 93% of 2016 federal wiretaps were directed against portable devices[93]—technology that in 1968 existed only on the Starship Enterprise.[94] This adaptation began with the courts and was accomplished with a revision to the Wiretap Act that added the word "electronic" to the list of prohibited communications interceptions.[95] The Wiretap Act remains a high bar, and wiretaps are still used only when absolutely necessary because of the time and effort it takes to obtain authorization for them.

Why has the Wiretap Act held up so well? First, its prohibition on interceptions is broad. Any interception of a communication traveling across a wire (or, after the Act was updated, on a radio, electromagnetic, photoelectronic, or photo-optical system) or an oral conversation made with the expectation of privacy is disallowed unless explicitly provided for by the statute. Second, the Wiretap Act's definition of what constitutes an interception is comprehensive, encompassing any acquisition of the contents of a communication through any device. The Act's broad and all-encompassing nature allows courts to apply it to new technologies without waiting for Congress to act. No matter how inventive law enforcement agencies are and no matter how different technology looks in the future, anything involving real-time interception of communications will continue to be protected.

ECPA and its updates, on the other hand, are much less comprehensive in relation to the field they intend to regulate; therefore, they have been much less successful at keeping up with rapidly evolving technology. ECPA sets aside specific categories of electronic information—stored electronic

---

[93] *See* Admin. Office of the U.S. Courts, *supra* note 69, tbl.2.

[94] *See* Paul Levinson, Cellphone: The Story of the World's Most Mobile Medium and How It Has Transformed Everything 31 (2004).

[95] *See, e.g.*, ECPA, Pub. L. No. 99-508, tit. 1, 100 Stat. 1848 (1986) (codified as amended in 18 U.S.C. § 2510(4)). After these revisions, Title III criminalizes the interception of "any wire, oral, or electronic communication." 18 U.S.C. § 2511 (2012). "Electronic communication" was defined broadly to "mean[ ] 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" with a few exceptions for already-defined communications. *Id.* § 2510(12).

communications (i.e., email) the data stored by remote computing services, and subscriber information—and provides them very limited protection. All other electronic information is unprotected the moment it is no longer in transit.[96] But in a world of cheap storage, retrieval is as much a concern as interception. ECPA nodded in this direction with its limited protection for the contents held by ECS and RCS providers, but a modern statute would need to be far more comprehensive to have any effect. ECPA was narrowly tailored for its time, which has ultimately been its undoing.

B. Multiple Types of Legal Process

One of the most common criticisms of ECPA is the multiple types of legal process introduced by the law. Not only are these standards confusing, but they also encourage law enforcement to push the boundaries of what information less-stringent types of legal process can be used to obtain about suspects. Kerr, for example, argues that a twenty-first century communications privacy law "should confer a single legal standard for access to the contents of data held by or for a customer or subscriber."[97] Kerr is correct that the legal process used to access communications should not depend on whether a business or individual holds the communication. He is also right that time and transmission technology are not a coherent way of differentiating content: whether law enforcement reads an email as it is being sent or several days later does not change the author and recipient's privacy interests in that email.

However, it does not follow that all law enforcement requests should be subject to the same standard of review or type of legal process. The privacy interest a customer has in the contents of a single email between herself and the suspect of a crime is fundamentally different than the one she has in the entire contents of her email account.[98] This distinction also applies to non-content data. The privacy interest a subscriber has in her phone number is very different than the one she has in the location of her cell phone at all times for the past six months. Different types of legal process should be kept precisely to allow for this differentiation. There are certainly times that police will require access to somebody's location history or the entire contents of their inbox, but they should face a high bar to access that information. Multiple types of legal process can make sense as long as the way they are assigned makes sense.

---

[96] While in transit, it is covered by the Wiretap Act itself, which after ECPA disallows contemporaneous interceptions of data transmissions. *See* ECPA tit. I; Kerr, *The Next Generation Communications Privacy Act*, *supra* note 23, at 382.

[97] *See* Kerr, *The Next Generation Communications Privacy Act*, *supra* note 23, at 411.

[98] *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (remarking that "'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life").

From a pragmatic standpoint, administrative subpoenas need to make up some part of the new scheme to appease the administrative agencies. During the 2013–2014 Congress, 272 members—well more than half—of the House of Representatives co-sponsored the Email Privacy Act. This Act would only have modified ECPA slightly by requiring a warrant to gain access to the contents of emails. The administrative agencies—especially the IRS and SEC, which rely on administrative subpoenas—vehemently opposed the bill, so the House leadership never scheduled a vote.[99]

C. Why act now?

The legal landscape is ripe for change. The Wiretap Act came about in part because the *Berger* and *Katz* decisions cast doubt on law enforcement wiretapping as it was then happening.[100] Congress responded to the decisions by passing an act that met and exceeded the Fourth Amendment minimums laid out by the Court. ECPA was the result of the *Miller* and *Smith* decisions along with a trailblazing report by the Office of Technology Assessment highlighting increased risks to privacy.[101] The *Warshak* decision paved the way for recent legislation to require law enforcement to obtain warrants to access emails. The third-party doctrine is also coming under increasing criticism in the Supreme Court.[102] And this Term, the Court is considering the propriety of warrantless access to large amounts of historic cell phone location information.[103] If Congress does not act soon, the Court may soon force its hand.

IV. Consistent and Comprehensive Application

Any overhaul of domestic law enforcement communications access should incorporate two components. First, as now, different types of legal process—each with its own standard of review—should apply to different law enforcement communications surveillance. What legal process applies to

---

[99] *See H.R. 1852 – Email Privacy Act*, Congress.gov (May 7, 2013), https://www.congress.gov/bill/113th-congress/house-bill/1852/cosponsors?q=%7B%22search%22%3A%5B%22Email+Privacy+Act%22%5D%7D [https://perma.cc/FUR9-NPR9]; Mike Masnick, *More Than Half of the House Co-Sponsoring Email Privacy Reform; So Why Isn't It Moving?*, techdirt (June 18, 2014, 12:07 PM), https://www.techdirt.com/articles/20140618/06573127610/more-than-half-house-co-sponsoring-email-privacy-reform-so-why-isnt-it-moving.shtml [https://perma.cc/JXP2-EPDB]; Kate Tummarello, *Bill Requiring Warrants for Email Searches Hits Magic Number in House*, Hill (June 18, 2014, 6:00 AM), http://thehill.com/policy/technology/209730-house-email-privacy-bill-hits-magic-number [https://perma.cc/8GSE-73J5].

[100] *See* Timothy Casey, *Electronic Surveillance and the Right to be Secure*, 41 U.C. Davis L. Rev. 977, 998–1000 (2008).

[101] Juan Williams, *Hill Study Says Privacy Laws Are Far Behind Technology: Authorized Surveillance at All-Time High*, Wash. Post, Oct. 24, 1985, at A14.

[102] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[103] *See Carpenter*, 137 S. Ct. at 2211.

what surveillance activity, however, should be based on a balance of the scope of that access against the sensitivity of what is accessed. Second, this overhaul should be comprehensive so that all domestic law enforcement access to communications fits somewhere within its scheme.

A. Consistent Legal Process Based on Scope and Sensitivity

All access to communications balances the needs of law enforcement against the privacy interests of individuals.[104] These competing interests have traditionally been expressed by the *Katz* test: a subjective expectation of privacy that society is prepared to treat as objectively reasonable. However, the increased availability of cheap storage combined with the pervasiveness of human-device interactions alters this landscape. In addition to objectively sensitive private information, seemingly insignificant and quasi-public information can become sensitive when aggregated.[105] So, in addition to protecting traditionally sensitive information, a comprehensive scheme should also provide some protection against overbroad collection of seemingly innocuous data by law enforcement.

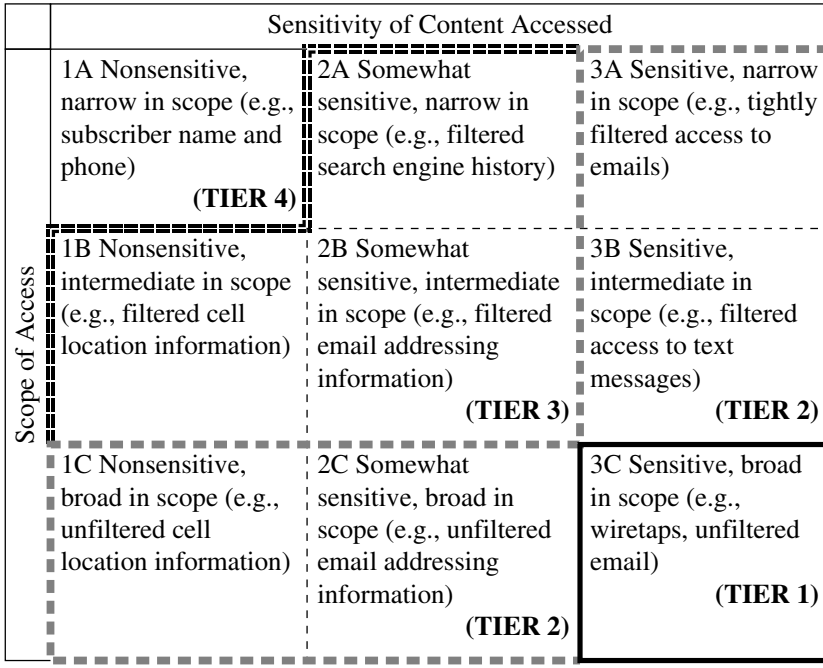
If all content and noncontent communication information is classified as 1) nonsensitive, 2) somewhat sensitive, or 3) sensitive and all requests for information as A) narrow in scope, B) intermediate in scope, or C) broad in scope, then there are nine possibilities ranging from 1A) nonsensitive and narrow in scope to 3C) sensitive and broad in scope. These nine possibilities can be broken down into four tiers reflecting the different types of legal process available. These possibilities are displayed in Figure 1 below.

---

[104] *Cf.* United States v. U.S. Dist. Court, 407 U.S. 297, 314–15 (1972) ("As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression.").

[105] *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (noting that public location monitoring can provide "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations"). And it is not just aggregation that erodes privacy. Even seemingly anonymous activities can be de-anonymized relatively easily through the use of large datasets. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1705 (2010) ("Reidentification combines datasets that were meant to be kept apart, and in doing so, gains power through accretion: Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification. Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal.").

FIGURE 1: CONTENT AND NONCONTENT COMMUNICATIONS INFORMATION



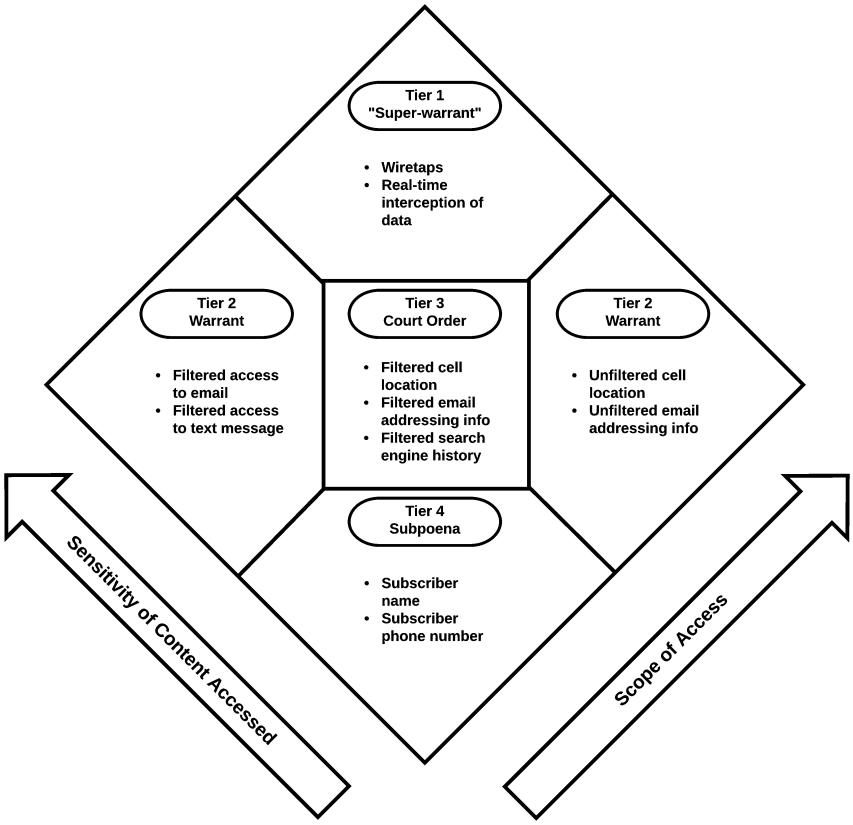
Requests for sensitive information that are broad in scope should be subject to the strictest review—call it Tier 1 review. Requests for nonsensitive information that are narrow in scope should receive the least restrictive review—Tier 4. In between these extremes, requests of narrow or intermediate scope for information that is sensitive along with broad requests for somewhat sensitive or nonsensitive information should receive a relatively high level of protection—Tier 2. Finally, requests that fall in between these categories because they are for somewhat sensitive information and are intermediate in scope should receive a lower-intermediate level of protection—Tier 3.

All domestic communications surveillance activities can be placed into one of these categories. Further, the existing types of legal process with established standards of review and case law can be grafted onto each of these tiers. Given the extreme privacy concerns involved, Tier 1 deserves super-warrant protection. Tier 2, which probably encompasses most domestic communications surveillance, should receive the protection of a warrant.[106] Tier

[106] Either an ECPA warrant or a traditional search warrant is appropriate depending on the type of material or information requested. The only difference between them is that a law enforcement officer need not personally execute an ECPA warrant, which still makes sense when the information requested is remote and digital.

3, which deserves some protection but does not involve sensitive information or broad requests, could be served by the equivalent of a § 2703(d) court order requiring specific and articulable facts. Finally, Tier 4, which is narrow in scope and nonsensitive, should be available by subpoena. A visual representation of these tiers, these types of legal process, and the sort of information that could fit in each can be found in the Figure 2 below.

FIGURE 2: TYPES OF LEGAL PROCESS BY TIER



Model for legal process in domestic law enforcement surveillance cases based on scope of access to information and sensitivity of information accessed.

The legislation establishing this tiered approach should specify where common content and information requests would fall on the new surveillance ladder. However, the comprehensive nature of this scheme is essential, as spelled out below. Therefore, these placements should be seen as guideposts rather than an exclusive list of where information and requests would fall on the ladder.

Tier 1, which receives the most protection, should be reserved for requests for sensitive information that are broad in scope. Everything covered

by the current Wiretap Act—telephone wiretaps, video and audio surveillance of private rooms, and live interception of all data transiting a computer—fall within this category because the unrestricted access is broad in scope, and a person's private conversations are potentially sensitive. Added to this tier is unfiltered access to a target's email, which is no less invasive than a wiretap and should be treated as such.

Tier 2, which requires a probable cause warrant, contains requests that are either for sensitive information or that are broad in scope. Sensitive information that is not broad in scope includes filtered access to the content of email or text conversations. "Filtered" access would include all messages exchanged between two suspects or all messages exchanged in the days surrounding specified criminal activity. Access to any communications stored on seized devices also fits within this category. This is true not only because a warrant has always sufficed for such searches but also because limiting access to the devices specified in a warrant necessarily limits the scope of the search.

Searches that are broad in scope but target only somewhat sensitive or nonsensitive data mostly consist of the aggregation of noncontent information. For example, unfiltered tracking data about a person's movements is not inherently sensitive because those movements are displayed in public, but the aggregation of that data does present privacy concerns.[107] Area signal interception is another example. The data collected—the name and phone number of all those using a particular cell site—is not particularly sensitive, but the broad scope of the inquiry raises privacy concerns. Finally, unfiltered access to noncontent data like real-time phone call records, lists of email "To" and "From" information, search engine history,[108] and website access logs fit here because of the expansive scope of such information when aggregated.

Tier 3, which requires a § 2703(d)-like court order contains requests for nonsensitive or somewhat sensitive information that is intermediate in scope and somewhat sensitive information that is narrow in scope. Filtered phone logs, filtered email "To" and "From" information, filtered search engine history, and filtered website access logs all fit within this category. The filtered content of messages posted on a Facebook wall also fits within this category because of the semipublic nature of such content and the narrow scope of filtering. Filtered cell location information fits here, too, because it is nonsensitive and intermediate in scope.

---

[107] *See Jones*, 565 U.S. at 414–17 (Sotomayor, J., concurring).

[108] Indeed, when AOL in 1996 publicly released 20 million searches and associated each search with a unique user ID, it did not take long for reporters accessing the data to start identifying specific users from the searches. Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, at A1; Charlie Savage, *What Can Be Gleaned from the President's Allegations on Twitter of Wiretapping*, N.Y. Times, Mar. 6, 2017, at A13 ("If it was a criminal wiretap, it would mean that the Justice Department had gathered sufficient evidence to convince a federal judge that someone using the phone number or email address probably committed a serious crime.").

Finally, Tier 4, which requires only a subpoena, contains requests for nonsensitive information that are narrow in scope. Subscriber and billing information (name, address, payment type used, IP address used to establish account) for a specific IP address, and an identified subject's phone number and email address all fit within this category.

B. Comprehensive Application to All Domestic Communications Surveillance

As simple as it is, the requirement that all domestic communications surveillance must fit somewhere within the framework laid out above is even more important than the arrangement of the framework itself. This comprehensive nature is what has allowed the Wiretap Act to endure while ECPA becomes more and more obsolete. It is also what separates this Note's proposals from those put forward by groups like the Digital Due Process Coalition, which suggest a pared down version of the new scheme laid out above but do not address making the changes comprehensive to cover existing and future forms of communication and associated data.[109] Any legislation enacting a new domestic communications surveillance framework must at least include language to the effect of the following, which is adapted from the Wiretap Act:[110]

> Except as otherwise specifically provided in this chapter any person who intentionally accesses, endeavors to access, or procures any other person to access or endeavor to access, any private communication or associated information without the consent of a party to the communication shall be punished as provided in subsection # or shall be subject to suit as provided in subsection #.
>
> Whenever any private communication or associated information has been intercepted, no part of the contents of such communication or information and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that communication or information would be in violation of this chapter.
>
> As used in this chapter—
> (1) "private" means not generally available to the public at large;
> (2) "communication" means the act or process of using words, sounds, signs, symbols, characters, behaviors, or any other medium to ex-

---

[109] *See About the Issue*, DIG. DUE PROCESS COAL., https://digitaldueprocess.org/about-the-issue/ [https://perma.cc/P39Q-LMKA].

[110] *See* 18 U.S.C. §§ 2510–2511 (2012).

press or exchange information, ideas, thoughts, feelings, and the like to another person;

(3) "associated information" means any facts or details pertaining to a communication that are private;

(4) "access" means the viewing, listening to, or acquisition of the contents of any communication or associated information through the use of any electronic, mechanical, or other device;

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to access a communication other than—
   a. any instrument, equipment, or facility or any component thereof,
      i. furnished to the subscriber or user by a provider of communications service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for use of the facilities of such service and used in the ordinary course of its business; or
      ii. being used by a provider of communications service in the ordinary course of its business, or by an investigative or law enforcement officer as authorized under this chapter;
   b. a hearing, visual, or other similar sensory aid device being used to correct subnormal perception to not better than normal;

(6) "communications service" means any service which provides to users thereof the ability to send or receive communications;

(7) "user" means any person or entity who—
   a. uses a communications service; and
   b. is duly authorized by the provider of such service to engage in such use;

(8) "party to the communication" means a person known by at least one other party to the communication to be accessing the conversation but does not include a communications service or the employees or agents thereof acting in the performance of their duties;

(9) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

Unforeseen change is the enemy of any supposedly comprehensive scheme, and this law enforcement domestic surveillance framework will not be successful if it cannot fit changing circumstances. The language above is very broad with the intent that it will cover all forms of communication.

V. Testing the Proposal

This Part applies the framework advocated by this Note to different forms of communications. First, the framework will be used to "backtest" a form of communication that courts have already dealt with under ECPA. Next, it will be applied to a hypothetical new form of communication. Fi-

nally, the framework will be used to analyze a service falling outside its ambit in order to demonstrate its limits.

A. Test Case 1: Facebook

Facebook is a social media platform with many components, but at its core Facebook is about communication. Therefore, if this Note's framework is successful, it will apply to law enforcement attempts to access Facebook material. Moreover, if the framework is superior to that currently in place under ECPA, it will apply in a more comprehensive and coherent way than does ECPA.

First, does the new domestic communications surveillance framework cover a law enforcement request for Facebook information? Looking to the text of the provision and assuming that law enforcement seeks access to private messages, wall posts, and the IP address from which a targeted user accessed her account, then the answer is yes. A user's private messages easily fit within the legislation's definition of "private communication" because these messages use words to exchange information and are not generally available to the public at large. The same is true for wall posts, which are used to exchange information and are only available to a limited group of the user's friends, though these are less private than private messages. Of course, some Facebook users open their wall for all to see. In that case, the communication would not be private and would not be covered by the framework. That is a correct result because a coherent communications surveillance framework would not put law enforcement at a disadvantage to a generic Internet user. Finally, the accountholder's IP address—while not a communication—is associated information because it is a fact that pertains to the accountholder's communication, and it is not available to the public at large.

Second, now that coverage is established, what form of legal process would law enforcement need to access each item? This depends on the level of access required. If law enforcement seeks complete access to all of a user's private messages, then it would need to obtain a super-warrant because the information contained in these messages is potentially sensitive, and total access to the messages is broad in scope, necessitating Tier 1 protections. If, on the other hand, law enforcement sought only messages between the user and the person with whom she was arrested robbing a bank, then that filtered content would drop the request into Tier 2 and require a warrant. Any posts between the two on each other's Facebook walls would receive Tier 3 protection and be accessible with a court order because the filtering by person reduces the scope of the information sought and the semipublic nature of a Facebook wall reduces the sensitivity of the information posted on it. Finally, if law enforcement sought every IP address from which the user logged on, that sort of unfiltered noncontent data would receive Tier 2 protection and require a warrant because the Internet address from which a user connects to a website is not particularly sensitive, but

access to many such addresses over a long period is broad in scope. On the other hand, if law enforcement sought only the IP address the accountholder used to establish the account or from which she most recently logged on, that information would receive Tier 4 protection and require only a subpoena because it is both nonsensitive and narrow in scope.

Third, is this process superior to ECPA? In one case applying ECPA to Facebook messages, a court held that if a Facebook private message has been opened and retained in a user's inbox, it was considered stored by a remote computing service and therefore could be obtained with only a subpoena.[111] Postings to the same user's Facebook wall were deemed analogous to Bulletin Board System postings contemplated by ECPA, so if access to that wall was limited, then those messages could not be obtained by subpoena because they enjoyed greater protection.[112] The case did not deal with an IP address request, but such requests are typically disposed of with subpoenas.[113] This Note's framework is superior to the court's ECPA application because there is no logical reason for a semiprivate wall post to receive more protection than a private message.

B. Test Case 2: Holograms

This next test case calls for some imagination, as it requires envisioning a new form of communication to which we can apply the framework.[114] In this case, the imagined technology is a holographic projection of a person that is beamed to Earth at the speed of light via a focused energy beam originating from a satellite in space.[115] Perhaps the person using this projection to communicate is up to no good as law enforcement wishes to intercept the communication. Doing so with a hidden microphone at the source or destination would clearly implicate the Wiretap Act, but what if law enforcement had some means of tapping into the directed energy transmission itself?

First, the tap would be covered under this Note's framework. The light beam is a communication because it is being used to exchange information. The law enforcement action counts as access because it entails using an apparatus to acquire the contents of that communication.

---

[111] *See* THOMPSON, *supra* note 60, at 11. Thompson discusses the application of ECPA to Facebook in a civil case, *see id.*, but the results would be analogous in a criminal matter.

[112] *Id.*

[113] *See Legal Process for User Data Requests FAQs*, GOOGLE, https://support.google.com/transparencyreport/answer/7381738?hl=EN [https://perma.cc/7038-AFEY] (stating that "[b]y far the most common" legal request Google receives from U.S. government agencies "is the subpoena," which can "compel [Google] to disclose . . . the IP addresses from which [a user] created the account and signed in and out (with dates and times)").

[114] If the author had a better understanding of such hypothetical technologies, he would be busy perfecting them instead of legal systems to regulate them.

[115] *See generally* GRAHAM SAXBY, PRACTICAL HOLOGRAPHY (3d ed. 2003) (describing the scientific and theoretical framework behind holograms).

Second, the interception of an entire conversation as it occurs is broad in scope and implicates potentially sensitive information, so this access would fall under Tier 1. Law enforcement would be required to obtain a super-warrant to access the material.

Third, this Note's framework is superior to current communications surveillance law because current law would likely not cover this tap at all. A directed light beam is not a "radio" communication under the Wiretap Act, nor is it oral, aural, or by wire. It might be an electronic communication, which includes transfers by "photoelectronic or photooptical system,"[116] but these terms remain undefined. Because the statute does not reach holograms, Congress likely would have to amend current law to cover these energy-based communications. The fact that the communications were being transmitted through the air likely would mean there was no reasonable expectation of privacy under *Katz*.

C. Test Case 3: Dropbox

Finally, to demonstrate the limits of this Note's framework, it will be used to analyze law enforcement action falling outside its purview. This Note's framework is not a replacement for the Fourth Amendment nor is it a comprehensive privacy statute for the digital age. It focuses on communications. Generally, Dropbox is a cloud-based file management system used for backup purposes. Files are not placed there as a means of communicating with others. Presuming a traditional use of Dropbox, law enforcement attempts to access the files a user stored in the cloud via Dropbox would not implicate this Note's proposals because that act of storage was not a communication.[117]

By contrast, Dropbox is a RCS under ECPA, so a Dropbox user enjoys the small amount of protection provided by requiring a subpoena. In this case, ECPA provides greater protection than this Note's proposed framework.

VI. Conclusion

The standards currently governing domestic law enforcement access to private communications are cumbersome, illogical, and ripe for change. Different scholars have proposed both narrow and broad changes to our current regime. This Note draws from and responds to these works with its own proposal for a new framework for law enforcement access to communications and related information. It calls for an end to legal requirements that treat the same categories of content differently based on where they were and what format they came in. But this Note also advocates that any new

[116] *See* 18 U.S.C. § 2510(12).

[117] Files sent between Dropbox users that are effectively emails would be treated as such.

framework maintain different levels of legal review because while all content is equivalent, not all requests for content are. In this vein, it proposes a four-tier system of review for surveillance actions, with those that are broad in scope and that involve sensitive information receiving the most scrutiny and those that are narrow in scope and that involve nonsensitive data receiving the least.

For this system to function long-term, this Note's second proposal is that it be enacted in a comprehensive way. Like the Wiretap Act, which has readily adapted to new technology within its domain, this act should broadly define communication so changes in how people communicate will not strip those communications of protection.

Now is the time for change. The public is conversant in the language of privacy. The Court is willing to consider the implications of a digitized world. Congress must act to bring the law governing law enforcement access to private communications into the modern age.

APPENDIX A: Communications Interception Chart for Federal Prosecutors (ca. 2003)[119]

INFO SOUGHT	DEVICE	PAPER NEEDED	STATUTE	AUTHORIZING OFFICIAL(s)	DURATION	STANDARD OF REVIEW
Phone Number Dialed- Real Time (outgoing)	Pen Register	Court Order	18 USC 3122, 3123	Magistrate	60 days	Relevance
Phone Number Dialed- Real Time (incoming)	Trap & Trace/ Caller ID	Court Order	18 USC 3122, 3123	Magistrate	60 days	Relevance
Incoming And Outgoing Phone Numbers Dialed And Subscriber Info- In Storage	Toll Records	Subpoena (grand jury or trial) Admin Subpoena Court Order	18 USC 2703(c)	Grand Jury/ Agency/ Magistrate		Specific And Articulable Facts (Relevant and material to an ongoing investigation) (Only if court order needed)
Cell Locating Information (tracking cell phones)	Pen Register/ Smart System	Court Order	18 U.S.C. 2703(d)	Magistrate	60 Days	Specific And Articulable Facts
Oral Communications	Bug	Title III	18 USC 2518	Dist Ct Judge and DOJ - DAAG/ OEO	30 Days (from 1st interception, or 10 days from signing)	Probable Cause+
Faxed Documents (real time)	Fax Machine (electronic communications)	Title III	18 U.S.C. 2518	Dist Ct Judge and DOJ- DAAG/OEO	30 Days	Probable Cause+
Computer Files/ Stored Or Down-Loaded/ Downloaded Emails	Computer Stand-Alone	Search Warrant	Rule 41 FRCP	Magistrate		Probable Cause
Computer Messages Sent Via E-Mail (Real Time Interception- Content)	Computer Network Intercept Device	Title III (if real-time interception)	18 USC 2518	Dist Ct Judge/ and DOJ- DAAG/OEO	30 days	Probable Cause+
Unopened Email (in storage - 180 days or less)	Internet Service Provider	Search Warrant	18 U.S.C. 2703(a)	Magistrate		Probable Cause
Unopened Email (in storage more than 180 days)	Internet Service Provider	Subpoena Court Order Warrant	18 U.S.C. 2703(a),(b)	Magistrate (if court order or warrant)		Specific And Articulable Facts (order) or Probable Cause (warrant)
Opened Email (still on service provider's system)	Internet Service Provider	Subpoena Court Order Warrant	18 U.S.C. 2703(b)	Magistrate (if court order or warrant)		Specific And Articulable Facts (order) or Probable Cause (warrant)
Email Subscriber Information/Transactional Information	Internet Service Provider	Court Order	18 U.S.C. 2703(c)	Magistrate		Specific And Articulable Facts
Wire Communications Over Fraudulent Phone	Cloned Cellular Phone (wire communications)[FN3]	Title III	18 USC 2518	Dist Ct Judge and DOJ- DAAG/OEO	30 days	Probable Cause+
Use Of Multiple Cellular Or Pay Phones, Calling Cards- changing so often that the phones cannot be identified	Roving	Title III	18 USC 2518(11)(b)	Dct Judge and AAG- Contact OEO	30 days	Probable Cause (must include facts reflecting that facilities changed to thwart interception)
Video (installed by agents in residence/ business)	Video- CCTV (Closed Circuit Television)	Rule 41 Search Warrant + Title III Req'ts	Rule 41 FRCP	Dct Judge and OEO (DOJ policy)	No More Than 30 Days	Probable Cause with Title III req'ts (Duration, Minimization, Necessity, etc.)
Video- camera already on premises	Security Camera- (already in place- need interception equipment to monitor	Title III (electronic communication)	18 USC 2518	Dist Ct Judge and DOJ- DAAG/OEO	30 Days	Probable Cause+
Video (outside premises- public area)	Pole Camera	No Warrant Needed (unless viewing protected area)[FN4]				
Names And Numbers From Electronic Address Book	Elec. Data note book Palm pilot	Search Warrant	Rule 41 FRCP	Magistrate		Probable Cause
tracking device - (location of target subjects or targeted item)	Transponder, Bumper Beeper, GPS (global positioning system)	Search Warrant[FN5]	18 U.S.C. 3117(a) and Rule 41 FRCP	Magistrate		Probable Cause
Identify Cell Phone By Electronic Serial Number (ESN) Or Phone Number (MIN)	Cell Site Simulator, Digital Analyzer (reads Electronic Serial Number and Phone number)	Court Order (if only ESN/phone number requested and search requires phone company's cooperation[FN6]	18 U.S.C. 2703(d)	Magistrate		Specific And Articulable Facts
Info From Seized Pager	Pager-Seized	Search Warrant (unless incident to arrest - then no paper needed)[FN7]	Rule 41 FRCP	Magistrate		Probable Cause
Realtime Intercept - Messages Sent To Pager (clone)	Pager -Cloned (electronic communication)	Title III	18 USC 2518	Dist Ct Judge; Don't Need DAAG/OEO APPROVAL	30 Days	Probable Cause+

[119] *Obtaining Electronic Evidence*, FED. LAW ENF'T TRAINING CTR., https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/downloads/other/obtaining_electronic.pdf [https://perma.cc/8BTE-4HLV].