Northwestern Journal of Technology and Intellectual Property

Volume 15 | Issue 1 Article 4

Spring 2017

A Mystery Wrapped in an Encryption: Surveillance and Privacy in the Encrypted Era

Shannon Gross
Northwestern University Pritzker School of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

A Mystery Wrapped in Encryption: Surveillance and Privacy in the Encrypted Era

Shannon Gross

May 2017 VOL. 15, NO. 1

Northwestern Journal of Technology and Intellectual Property
Volume 15, Number 1 (2017)

A Mystery Wrapped in an Encryption: Surveillance and Privacy in the Encrypted Era

By Shannon Gross*

* Northwestern University Pritzker School of Law, J.D. candidate, 2017

ABSTRACT

¶1 *At the moment, there is a debate between law enforcement and the technology industry, on behalf of their users, about the whether technology companies should provide backdoors or assistance when users encrypt their communications. Despite the needs of law enforcement, backdoors or other unlocking measures can severely intrude into consumer privacy interests. At the risk of losing evidence, privacy should be the dominant concern, which has been supported by the Supreme Court noting that "privacy comes at a cost".*[1] *Stephanie Pell and others have discussed the problems with current statutes for privacy interests, but the discussions surrounding encryption technology are a new issue that has not been closely covered by legal scholarship. This note uses a privacy rights analysis to support technology companies' arguments for noncompliance with law enforcement requests to de-encrypt encrypted communications. As the debate continues ahead, this note may provide support for consumer privacy against law enforcement intrusion.*

[1] Riley, 134 S. Ct., at 2493.

TABLE OF CONTENTS

INTRODUCTION

¶2 Imagine a police investigation. The police believe they will have a chance to apprehend their target at a large sale they know through informants is going to occur shortly. The police do not know the exact time and location of the sale, however. They attempt a wiretap on the cell phones of relevant actors, but no information can be gleaned from the wiretap. No one is using text messages, no phone calls regarding the sale come through. The police believe the targets are using a service that encrypts their communications, something as simple as iMessage on Apple products or the Skype application on their phones. Running out of time, the police contemplate a warrant. Do they get a warrant for the company, such as Apple, to turn over all communications from certain accounts, or instead for the phones themselves? The company may reply they are unable to comply with the warrant because the encryption also prevents the company itself from retrieving information. So, the police are left to retrieve the phones themselves, tipping off their targets that law enforcement is involved either through notice to the owner of the phone or through an in-person search; likely preventing the very event necessary for the arrest of their target, if it had not already occurred by the time they were able to get warrants for the phones.

¶3 This situation highlights the current battle between effective law enforcement and the right to privacy to one's own communications. The issue has begun to arise more often as technology companies, led by Apple and Microsoft, increasingly turn to encryption to protect their users.[2] For the moment, the Trump Administration has decided not to force compliance, although the issue remains hotly debated between the government and law enforcement,[3] especially as the debate gained more coverage after Apple refused to decrypt the phone of one of the shooters in the San Bernardino massacre[4]. The wiretapping statues do not govern encrypted communications that run through technology companies rather than phone companies, such as iMessage, Skype, or WhatsApp. Technology companies do not always comply with wiretapping requests or warrants, either because the relevant statute, the Communications Assistance for Law Enforcement Act (CALEA), does not cover the communications or because the companies are unable to comply due to encryption.

¶4 American law at the moment has not caught up with our current technology boom, leading to a unique gap in case law. While wiretaps for technology companies remain

---

[2] *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), http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html [https://perma.cc/VYE5-G7DA]. *See also*, Ellen Nakashima & Barton Gellman, *As encryption spreads, U.S. grapples with clash between privacy, security,* WASH. POST, (April 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html [https://perma.cc/3ENN-MAUS].

[3] *See* Nicole Perlroth & David E. Sanger, *Obama Won't Seek Access to Encrypted User Data,* N.Y. TIMES (Oct. 10, 2015), http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html [https://perma.cc/7H9K-WLF6].

[4] *See* Marie Andrusewicz, Apple Opposes Judge's Order To Help FBI Unlock San Bernardino Shooter's Phone, NPR (Feb. 17, 2016), http://www.npr.org/sections/thetwo-way/2016/02/17/467035863/judge-orders-apple-to-help-investigators-unlock-california-shooters-phone [https://perma.cc/H7ZY-8SDC].

difficult to pursue, there is a growing body of case law regarding tech companies' compliance with warrants for phones, entire email accounts, Facebook profiles, and other communicatory services. So far, the courts have generally ruled in favor of law enforcement to the detriment of privacy rights, contractual agreements between the companies and users, and congruence with international law.

¶5 This comment will address this gap in the law, and argue that privacy concerns should govern the discussion regarding government access to communications. Section One contains a primer on the right to privacy in the United States and its importance. Section Two will introduce the relevant statutes required for wiretaps and warrants, the Electronic Communications Privacy Act (ECPA) and the Communications Assistance for Law Enforcement Act (CALEA). The section will explain their purpose and also address the Acts' privacy rights shortcomings. Section Three will address the current circuit split emerging over whether to issue warrants for items that include encrypted communications, such as entire cell phones, or Facebook and email accounts. It will argue that the split should be decided in favor of privacy rights, and that the dangers in turning over all of a person's communications outweigh the benefits even when there may be information helpful to a criminal investigation. Section Four will discuss the reasons why wiretaps for encrypted communications are not currently permitted or executable in the United States. Section Five will synthesize the previous sections, addressing how the law treats encrypted communications differently based on the type of surveillance. Finally, Section Six will offer predictions about where the law around encrypted communications is headed, and recommendations regarding the direction in which it should go.

I. THE RIGHT TO PRIVACY

¶6 The right to privacy in the United States derives from several sources, but is most strongly supported for the purposes of this paper by the Fourth Amendment, which states:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the person or things to be seized.[5]

The right to privacy in the Fourth Amendment is the right for citizens to have their bodies and their things "secure" or remaining theirs, unless the search is reasonable. So, while there is room for the government to access citizens' "persons, houses, papers, and effects," it must be reasonable.[6]

¶7 The Supreme Court has spent much time defining what a reasonable search and seizure is, and have shown through their decisions that privacy rights are to be taken

[5] U.S. CONST. amend. IV, cl. 1.
[6] *Id*.

seriously, and not disregarded in favor of public safety. Privacy rights are given precedence because they "impact[] fundamental values of a free society, such as freedom of speech, association, and expression."[7] The court has emphasized privacy rights in its Fourth Amendment jurisprudence, stating "[t]he security of one's privacy against arbitrary intrusion by the police — which is at the core of the Fourth Amendment — is basic to a free society."[8] In fact, Justice Roberts suggested privacy was an essential reason for the American fight for independence from Britain in *Riley v. California,* stating:

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself.[9]

Simply stated, the Court looks to privacy interests first, not to governmental interest.[10] The Court upholds this, even knowing that at times important evidence may be lost:

> "our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."[11]

The result is that even though privacy rights and law enforcement interests are weighed in a balancing test in Fourth Amendment procedure, privacy concerns are paramount and should only be invaded in rare circumstances.

¶8 The need to weigh more heavily on privacy interests is perhaps more important now than it ever has been, because of the sheer amount of information that is stored on cell phones. A single object such as a cell phone can provide access to a person's communications, location data, purchases, and any other activity conducted using that technology. The access to this data needs to be limited in a meaningful way, for the alternative is to have increased governmental invasion into the private sphere. The government has responded in various ways to the increased need for delineation of

[7] Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 KAN. L. REV. 235, 257 (2015).

[8] Wolf v. Colorado, 338 U.S. 25, 28 (1949).

[9] Riley v. California, 134 S. Ct. 2473, 2492 (2014).

[10] Weeks v. United States, 232 U.S. 383, 393 (1914) ("If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the Fourth Amendment declaring his right to be secure against such searches and seizures is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution. The efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great principles established by years of endeavor and suffering which have resulted in their embodiment in the fundamental law of the land.").

[11] *Riley*, 134 S. Ct., at 2493.

privacy rights. For example, the Obama Administration was the first to "explicitly support comprehensive privacy legislation."[12] The Federal Trade Commission has also become more interested in protecting privacy, requiring that major technology companies like Facebook sign privacy consent decrees.[13]

¶9 Privacy law is essential to a functioning democracy, as it allows freedom of speech and "is basic to a free society."[14] This paper claims privacy should be the governing interest because it is so fundamental to the functioning of American society.

II. CONGRESS' RESPONSE TO TECHNOLOGICAL ADVANCES IN THE ECPA AND CALEA

A. ECPA

¶10 The Electronic Communications and Privacy Act was passed in 1986, in response to the advance of technology.[15] The Act contains three sections: the Wiretap Act, the Stored Communications Act, and the Pen Register Act.[16] Prior to the Act's passage, a series of Supreme Court cases, the 'business records cases,' held that disclosure of personal information to businesses was outside the scope of Fourth Amendment privacy protection.[17] This was problematic with the advent of email and other services, as electronic communications require the user to share their information with the company providing the service. In fact, the user may have to share their information multiple times as it passes through different services, making a contemporaneous record of the communication (as opposed to a phone call which is not replicable).[18] With this risk to privacy in mind, Congress passed the Act.

¶11 However, as technology has progressed, the Act has not protected privacy as much as planned, because Congress focused on the different technologies operating at the time rather than the common privacy interests they all shared.[19] As others have argued, these acts need to be reformed to address the advent of technology in the modern age.[20] However, until that occurs, scholars and judges must use the statutes as they can to protect privacy interests.

¶12 Two of the sections, the Wiretap Act and the Pen Register statute, protected electronic communications in transit to some degree, but left broad authorizations such as

---

[12] Peter Swire, *Social Networks and the Law: Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1382 (2012).

[13] *Id*.

[14] *Wolf*, 333 U.S., at 8.

[15] Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977 (2008).

[16] 18 U.S.C. § 3127.

[17] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1562 (2004).

[18] *Id*. at 1562-63.

[19] Robert Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. TECH. L. REV. 1, 1 (2003).

[20] *Id*. at 5.

allowing interceptions based on any federal felony.[21] Earlier communications statutes restricted wiretaps only to certain crimes, but the ECPA has a much broader reach for law enforcement and "the ECPA contains no statutory exclusionary rule for wrongfully acquired electronic communications."[22] An exclusionary rule for wrongfully acquired electronic communications allows one to suppress evidence from unlawful searches and seizures; its absence from the ECPA burdens the suppression process.[23] Even still, the Wiretap Act has strong protections for electronic communications while they are in transit, extending the protections of Title III of the Omnibus Crime Control and Safe Streets Act, such as requiring a warrant before interception.[24] These sections are not as relevant to the analysis of encrypted communications as the Stored Communications Act (SCA), so this comment will focus on that portion of the ECPA.

¶13 The Stored Communications Act is part of the Electronic Communications Privacy Act, passed in 1986.[25] The SCA was passed in part to limit the government from requiring disclosure from third party providers of online services,[26] although it also identifies when law enforcement may gain access to stored communications.[27] The Act creates two categories of providers: Electronic Communication Service (ECS) providers give users the ability to send or receive wire or electronic communications, and Remote Computing Service (RCS) providers give users computer storage or processing services through electronic communications.[28] If the provider is either an ECS or a RCS provider, the government may access the communication through a search warrant without notice to the user, or give notice to the user and get the communications through a subpoena.[29] If a third party is in neither category, then the communication cannot be disclosed.[30] Today, most third parties are in neither category, as they typically provide elements of both categories to their users.

¶14 Since the Act was passed, the difference between these two categories has eroded, as most modern technology provides both services.[31] Neither ECS nor RCS providers may disclose data in electronic storage, but the government may obtain electronic communications in storage with ECS for less than 180 days through a warrant.[32] The Act does not require that the warrant outline the specific types of messages desired.[33]

¶15 For communications stored more than 180 days, the government can compel disclosure through a search warrant, or a combination of a subpoena (administrative or

---

[21] Mulligan, *supra* note 16, at 1566.

[22] *Id*.

[23] Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law,* 54 HASTINGS L.J. 805, 824 (2003).

[24] Mulligan, *supra* note 16, at 1562.

[25] Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 375 (2009).

[26] Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563, 566 (2011).

[27] Patricia Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1413 (2004).

[28] Scolnik, *supra* note 24, at 376.

[29] Bellia, *supra* note 26, at 1416.

[30] Ward, *supra* note 25, at 567.

[31] Scolnik, *supra* note 24, at 376.

[32] *Id*.

[33] *Id*. at 377.

grand jury), with prior notice to the user.[34] They may also get the information through notice to the user and a court order authorized by 18 U.S.C. § 2703(d), which has a reasonable suspicion standard for the believed relevancy of information sought, which is lower than the Fourth Amendment probable cause standard.[35] Some argue that the SCA unintentionally provides that companies like Facebook disclose all content as long as there is a subpoena, with less than probable cause.[36]

¶16 Stephanie Pell, a leading researcher in the area of government surveillance and technology, argues that in spite of a general consensus that the SCA is out of date, the legislature has been unable to pass a more modern act because they have not had accurate information about the type of surveillance the government has used in secret.[37] For example, Congress has never authorized StingRay technology, which is used by law enforcement to obtain detailed information of the location of cell phones without collaboration with wireless companies.[38] Congress cannot update surveillance statutes properly because they do not always receive notice of new surveillance methods and technologies being implemented by law enforcement.[39]

B. CALEA

¶17 The Communications Assistance for Law Enforcement Act (CALEA) determines the duties for telecommunications companies when they intercept communications at the request of law enforcement through wiretaps and other means, but CALEA does not determine the scope of government power to intercept communications.[40] The companies must provide the materials to allow the government to intercept wire and electronic communications.[41]

¶18 Voice Over Internet Protocol (VoIP) communications came under the purview of CALEA after traditional telephone systems started switching to VoIP and the FCC broadened the Act.[42] VoIP communications differ from the traditional systems because the information is separated into packets, without requiring the circuit between the source and the destination to be predetermined, or all the information to be sent through one

---

[34] Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 360 (2011).

[35] *Id*.

[36] *Id*.

[37] 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, 154 (2014).

[38] *Id.* at 142.

[39] *Id.* at 143.

[40] Barbara J. Van Arsdale, Annotation, *Construction and Application of Communications Assistance for Law Enforcement Act (CALEA)*, 47 U.S.C.A. §§ 1001 to 1010, 25 A.L.R. Fed. 2d 323 §2 (2008).

[41] *Id*.

[42] *See* Christa M. Hibbard, *Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance*, 64 FED. COMM. L.J. 371, 375 (2012).

switch.[43] CALEA was originally written for companies to intercept calls at a single switch between the responder and the caller, so the separation of the data would have thwarted wiretaps until CALEA was updated.[44]

¶19 However, when CALEA was broadened to include VoIP, other internet communications were intentionally kept out of the scope of the act.[45] While the FBI would like to expand CALEA to apply to internet communications providers, it would be difficult for companies to comply for several reasons. The first is that the internet as a structure would be difficult to create wiretap technology for, given its decentralized nature[46]. Wiretap technology was created for the organized and relatively uniform telecommunications industry, and the design of the internet does not map with wiretapping technology as it currently exists.[47] The second reason is that privacy rights would be at risk[48]. The way information is sent through the internet makes it hard to get particularized information specified in a warrant or wiretap order, increasing the likelihood that unauthorized information may also be discovered, especially since people tend to release private information on the internet.[49]

¶20 Constance Martin has explained CALEA's difference from other legislation as "not simply authoriz[ing] electronic surveillance . . . but requir[ing] telecommunications operators to take any necessary measures to aid law enforcement."[50] Martin advocates that CALEA was not intended for companies providing information services and that extending CALEA to the internet went against both the language of the act and privacy rights.[51] She argues the legislative intent was a narrow statute "focused on traditional phone lines," and that internet and VoIP services should be exempt from CALEA.[52]

¶21 In sum, CALEA and the EPCA work together to enable law enforcement to look into communications, although with varying levels of success and protection to citizens. Because both statutes were enacted prior to the current age, they are ill fit for use either by the citizen to protect their rights, or by law enforcement to conduct surveillance. These gaps in the statutory law allow for different interpretations of what rights people have in regards to their internet communications, which are addressed in the following section.

---

[43] Timothy Singleton, *Big Brother Hears You, But Can He Understand What He Hears? The Problematic Application of CALEA to VoIP Communications in the Age of Encryption,* 15 TULSA J. COMP. & INT'L L. 283, 287-88 (2008).

[44] *Id*. at 286.

[45] Hibbard, *supra* note 41, at 376.

[46] *Id*. at 384.

[47] *Id*.

[48] *Id*. at 385.

[49] *Id*. at 386-87.

[50] Constance L. Martin, *Exalted Technology: Should Calea Be Expanded to Authorize Internet Wiretapping*?, 32 RUTGERS COMPUTER & TECH. L.J. 140, 144 (2005).

[51] *Id*. at 156.

[52] *Id*. at 157, 180.

III. THE EMERGING CIRCUIT SPLIT OVER WARRANTS FOR ENCRYPTED COMMUNICATIONS

¶22 There is a split of authority emerging about whether warrants can be issued for an entire phone, or an entire email account. Some courts believe that law enforcement is not asking for access with sufficient particular language, but in many cases the issue does not come up at all and warrants are issued without comment from the court. Courts are being too cavalier with people's privacy rights when they grant such generalized warrants, as advances in technology should not reduce privacy protections.[53]

This issue was recently tried at the appeals level for the first time in the *Microsoft* case and the court would not order the warrant and it is important later cases continue to consider all the interests involved.[54] People's phones, email accounts, or Facebook profiles contain much more than possibly relevant evidence. They contain private financial information, health data, a multitude of personal communications, personal thoughts, and more. The Supreme Court, in *Riley v. California,* indicated that cell phones deserve extra privacy protections, and cannot be searched without a warrant because cell phones hold the "sum of an individual's private life," rather than just isolated bits of information like in times past.[55] In light of the Supreme Court's rationale in *Riley*, lower courts should give cell phones increased privacy protections, by ensuring that warrants that are issued are *specific*, since so much information is held on cell phones that should not be easily accessible by law enforcement with probable cause only of drug trade, for example. Pursuit of information regarding a drug deal should not allow access to private photos, medical apps, or any other private information unrelated to the drug charge. This is in keeping with past Supreme Court jurisprudence protecting residences due to the amount of private information that may be held in a home[56], analogous to a phone or email account in today's technological world.

A. Judges Grant Warrants for Encrypted Communications when they Consider the Cost to Technology Companies

¶23 Despite *Riley*, some courts have granted warrants for encrypted communications on suspects' devices, even over challenges from the companies that host the communications. Law enforcement is granted complete access to an entire account, when the warrants should be denied based on vagueness. The Fourth Amendment demands that

---

[53] *See* Berger v. New York, 388 U.S. 41, 49, (1967) ("The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge. This is not to say that individual privacy has been relegated to a second-class position for it has been held since Lord Camden's day that intrusions into it are 'subversive of all the comforts of society.'") (discussing advances in wiretap technology).

[54] In the Matter of Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 201 (2d Cir. 2016).

[55] *Riley*, 134 S. Ct., at 2495.

[56] *See* United States v. Karo, 468 U.S. 705, 714, (1984) ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.").

warrants have "particularity."[57] The Supreme Court has stated that particularity requirement in part, means that "warrants shall particularly describe the thing to be seized [to make] general searches under them impossible and prevent[] the seizure of one thing under a warrant describing another."[58] Therefore vague warrants that do not set out the content of messages or communications law enforcement believe will be present should be denied.

¶24 For example, Facebook challenged a trial court ruling that it could not litigate the constitutionality of warrants on its customers' behalf.[59] The state had issued 381 warrants for Facebook users suspected of Social Security fraud.[60] The appeals court upheld the trial court ruling, saying that no party, including Facebook, had the right to quash a warrant before it was issued.[61] The court rejected Facebook's argument that because the company was the one who had to retrieve the information, the warrant was more akin to a subpoena, which could be contested before it was carried out.[62] The court said this would cause any nontraditional search warrant to be unworkable.[63] While the court was concerned about privacy rights, the court determined that Facebook could not gain more rights than a citizen, and that any evidence gained from the warrants could be suppressed at a later time, rather than quashed pre-enforcement.[64]

¶25 In another case with a similar outcome, the court evaluated whether a warrant for an entire email account hosted by Gmail was overbroad and concluded it was not.[65] The court looked to case law on warrants for entire hard drives, and found that the same principles supported warrants for email accounts.[66] The court also rejected the notion that Google, as the host, should determine which emails were relevant to the warrant.[67] They believed the burden would have been too much for the company, and the simple solution was to have entire Gmail accounts sent to law enforcement to comply with warrants.[68] The court explicitly disagreed with other circuits, stating that the case law supported the government's warrant for an entire email account

¶26 The Facebook and Gmail cases are helpful to illustrate why courts are disregarding established privacy rights in favor of surveillance law. Courts are concerned with how relevant information will be determined from these sources, and do not want to burden technology companies with sorting through the mass of information that might be relevant to an investigation. This would be an unnecessary expense on business, and could make companies less willing to work with law enforcement if they were required to

---

[57] U.S. CONST. amend. IV, cl. 1.

[58] Marron v. United States, 275 U.S. 192, 196 (1927).

[59] *In re* 381 Search Warrants Directed to Facebook, Inc., 132 A.D.3d 11, 13 (N.Y. App. Div. 2015).

[60] *Id*.

[61] *Id*. at 18.

[62] *Id*. at 18-19.

[63] *Id*. at 19.

[64] *Id*. at 23.

[65] In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386, 386 (S.D.N.Y. 2014).

[66] *Id*. at 394.

[67] *Id*.

[68] *Id*. at 394-96.

expend dollars in order to comply with privacy law. The courts also rely on the law of evidence to protect privacy rights, stating that wrongly discovered information can be later quashed.

¶27 The problem with this reasoning is that it assumes that the problems are not the warrants themselves. A general warrant for an entire email account, without specifying what type of communications law enforcement is looking for, will be very difficult to later quash evidence from. The courts should be denying these types of warrants based on vagueness. While a technology company may not be able to sort through an entire account for the types of communications law enforcement is looking for, a particularized warrant would at least make it obvious what can later be deemed as outside the scope of a warrant. The danger is that there is no privacy when entire accounts are available to law enforcement to find evidence without any parameters.

B. Judges Deny Warrants for Encrypted Communications if they Fear Loss to Privacy Rights and Overbroad Warrants

¶28 Some courts recognize the danger to privacy, and have been denying overbroad warrants for encrypted communications. This is the desired outcome for privacy interests, as it encourages particular warrants, and reminds law enforcement that they do not have access to an individual's entire life or every communication.

¶29 In another case, the government sought warrants from "Google, Inc. ("Google"), GoDaddy, Verizon Internet Services ("Verizon"), Yahoo!, and Skype (collectively, "Providers"), to disclose copies of electronic communications — including the contents of all emails, instant messages, and chat logs/sessions" regarding a suspect in an interstate stolen property case.[69] The court determined that emails should receive Fourth Amendment protection, following the logic of case law that provided that warrants were still required for letters when they were handed to third party mail carriers, or phone calls which require a third party to transmit them.[70] The court then found that the warrants were too broad because they failed to set any limits on the information they were asking for and they violated the Fourth Amendment.[71] The court held the warrant "is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime."[72]

¶30 In another case, the district court rejected a warrant requesting to search a lawfully seized cellular telephone, in part because the warrant requested indefinite storage of encrypted data.[73] The court worried that the government could then store an iPhone

[69] *In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *1 (D. Kan. Aug. 27, 2013).

[70] *Id*. at 3-4.

[71] *Id*. at 8.

[72] *Id*.

[73] *In re* Nextel Cellular Tel., No. 14-MJ-8005-DJW, 2014 WL 2898262, at *11 (D. Kan. June 26, 2014); *see also*, *In re* Cellular Telephones, No. L4-MJ-8017-DJW, 2014 WL 7793690, at *6 (D. Kan. Dec. 30, 2014)(arguing that warrants for entire cell phones without a search protocol "would give the government carte blanche to examine the entirety of an individual's digital presence with impunity").

owner's "entire correspondence via iMessage indefinitely, much of which may lack probable cause having no connection to the crimes being investigated."[74]

¶31 Finally, illustrating the lack of consensus on these types of issues, a different district court in New York initially declined to issue an order requiring Apple to disable the encryption key on a suspect's iPhone.[75] While the court asked Apple to submit a memo regarding if compliance with the order would be unduly burdensome, the language of the order suggested they were hesitant to force Apple to comply.[76] The court stated that Congress is aware that there is a statutory gap in CALEA that prevents law enforcement from forcing compliance with these types of orders, but that Congress has not responded with any statutory update.[77] Also, the court was sensitive to Apple's motivations to satisfy its consumers and their interests in personal privacy and data security.[78] The court echoed these arguments in its ultimate order, deciding not to issue the order.[79] The court's analysis shows that some courts are properly weighing the right to privacy and companies' duty to respond to that need, rather than immediately deferring to law enforcement. Further, Apple will probably be unable to comply with this order, as they have argued in the San Bernardino case discussed below, as encryption purposefully keeps information from the technology companies as well as others – its purpose is to make information or communications impossible to access by anyone except the user.

IV. WIRETAPS FOR ENCRYPTED COMMUNICATIONS – A DISPUTED ISSUE

¶32 There is not a lot of case law on this issue, because law enforcement does not pursue wiretaps it cannot intercept.[80] Therefore, there is currently a gap in authority surrounding this issue, until there is statutory authority allowing or disallowing wiretaps of encrypted communications. This section will explain why law enforcement is unable to get wiretaps for encrypted communications, including technological hurdles, company resistance, and Constitutional law.

A. Technological Difficulties to Intercept Live Encrypted Communications

¶33 Even determining where to set up a wiretap for a Voice-Over Internet Protocol (VoIP) call is difficult. First of all, there is no way to determine exactly what ISP the caller and receiver are calling from, since it would change depending on their locations.[81] Even if that was possible, the ISPs cannot read the encrypted traffic of the VoIP call, so

[74] *See Nextel*, 2014 WL 7793690, at *11.
[75] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15MC1902, 2015 WL 5920207, at *1 (E.D.N.Y. Oct. 9, 2015).
[76] *Id*.
[77] *Id*. at *3.
[78] *Id*. at *6.
[79] *In re* Apple, Inc., 149 F. Supp. 3d 341, 360 (E.D.N.Y. 2016).
[80] Steven M. Bellovin et. al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 13 (2014).
[81] *Id*. at 10.

no information would be transmitted.[82] The VoIP providers may be in a different jurisdiction, and are unable to see what traffic they provide.[83] Therefore, even if the government wanted to extend CALEA to internet communications, it would be extremely difficult for the technology companies to be able to provide the infrastructure for wiretaps.

¶34 Bellovin argues that even as technology improves, most criminals do not use encryption, so fear of missing information is misplaced.[84] However, he cautions that if the Skype architecture, in which there is end-to-end encryption with no middle man, becomes prevalent with other services, then wiretapping would become very difficult.[85] Even Skype can provide location services, though, so law enforcement could gain some information from Skype or Skype-model companies.[86]

¶35 Stephanie Pell offers a similar perspective, saying that the government has issues "with wiretapping capabilities, not a lack of the legal authority to conduct surveillance".[87] There is no way to execute even a court-authorized wiretap for many of the encrypted communications companies, because the companies "lack[] the technical capability to implement" them, so law enforcement wants the legislature to encourage internet communications companies not under CALEA's purview to create interception capabilities in their products.[88] However, after Edward Snowden's disclosures, Congress is trepidatious to support surveillance, and law enforcement agencies are without a legal outlet to get live information from internet companies not under CALEA.[89]

B. Technology Companies' Increasing Reliance on Encryption

¶36 The technology companies also seem to want to distance themselves from law enforcement, most notably through making encryption a default setting.[90] Apple and Google have made encryption default on their cellular phones, and one imagines many other technology companies will follow suit.[91] The result is that providers do not have the information that law enforcement seeks, even if there is a search warrant or wiretap. As the cases above show, these companies are also fighting law enforcement in court, arguing on behalf of their users' rights to privacy.

---

[82] *Id*.
[83] *Id*.
[84] *Id*. at 15.
[85] *Id*.
[86] *Id*.
[87] Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix-Doctrine to Follow*, 14 N.C. J. L. & TECH. 489, 538 (2013).
[88] Jason M. Weinstein, William L. Drake, Nicholas P. Silverman, *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729, 748-49 (2015).
[89] *Id*. at 749.
[90] *Id*. at 744.
[91] *Id*.

V. WHY DOES THE LAW TREAT ENCRYPTED COMMUNICATION DIFFERENTLY BASED ON THE TYPE OF SURVEILLANCE?

A. Differences Between Wiretaps and Warrants for Encrypted Communications

¶37 Even before encrypted communications are implicated, there are substantial differences between wiretaps and warrants. First of all, the scope of the searches are different. A warrant application must show probable cause that the items will be found in the location listed and allows a single search of the location.[92] A wiretap must show probable cause that specific communications in the future will be seized through a specific telephone (or piece of technology), which allows law enforcement to listen as many times as necessary for up to thirty days.[93]

¶38 The main difference is that the wiretap is unachievable with the current state of technology, and the warrant may be able to give law enforcement information. However, if the government is getting a warrant to receive the information from the tech companies, the companies may not have access to the information sought because of encryption. So, the only way law enforcement may then get access to the information would be to examine the device the communications were sent from, if possible.

B. Similarities Between Wiretaps and Warrants for Encrypted Communications

¶39 Clifford Fishman argued that when law enforcement are issued warrants, "they usually know as soon as they see an object whether it falls within the ambit of items subject to seizure. If the police seize items not specified in the warrant or found in plain view, such items are not admissible in evidence."[94] On the other hand, when law enforcement use wiretaps, they are not able to tell whether the conversation is relevant to the investigation immediately, or even part-way through.[95]

¶40 In our current climate where warrants for entire email accounts or phones are granted in some states without thought, this distinction that Fishman describes is wearing down. Law enforcement will not be able to tell immediately what is relevant to their investigation if they are searching through an entire phone. There will be significant information that will not be relevant, but will be highly personal to the suspect. The same problems with privacy that concerned scholars in the 1970s now apply not only to wiretaps, but to warrants as well.

¶41 Law enforcement is able, without knowing specifically whether a message will be relevant, to peruse an entire email account, the equivalent of listening to every conversation a suspect might have. While a wiretap may overhear some private conversations, law enforcement officers must stop listening if the conversation is not pertinent to the investigation, as per the minimization provision in Title III of the

[92] Clifford S. Fishman, *The "Minimization" Requirement in Electronic Surveillance: Title III, The Fourth Amendment, and the Dread Scott Decision*, 28 AM. U. L. REV. 315, 317-18 (1979).
[93] *Id*. at 318.
[94] *Id*.
[95] *Id*.

Omnibus Crime Control and Safe Streets Act of 1968, which gives law enforcement the right to wiretap but also constrains their ability to do so.[96] However, in the situation of an email account or phone messages, law enforcement may open a message and immediately tell it is not relevant; but the act of opening the message is a breach of privacy in that they become privy to information they would not have received otherwise. Unlike a phone call in which they would have stopped recording when a suspect was having a conversation that was not relevant, they have access to the entire email or message as soon as it is opened, regardless of its relevance. Even if a similar constraint was instituted to written communications (i.e. the first 3 lines of the email must be relevant to the investigation), there is no way to ensure law enforcement would stop reading after that point, unlike a recording which requires clear action on the part of the officer. We are no longer only in the realm of search warrants for items, now warrants open up people's private thoughts and ruminations to law enforcement investigators.

VI. WHERE DOES THE LAW GO FROM HERE?

A. Predictions

¶42 Weinstein and his co-authors suggest that defense lawyers are in a unique position with regard to wiretaps and warrants for evidence "collected using digital means."[97] Defense lawyers could move to suppress a wiretap for an internet company, arguing also that the evidence underlying the wiretap, such as location information, should not be admitted.[98] Warrants for email accounts or cell phones can be attacked based on scope.[99]

¶43 Companies have also been litigating on behalf of their users and their privacy. In the *Microsoft* case, a search warrant was issued to Microsoft for records for a specific email account, but Microsoft moved to vacate on the premise that the warrant authorized a search and seizure of content stored in Ireland.[100] The district court determined that the court order giving the warrant was not a final order and therefore Microsoft could not appeal it so their case was "defective at this stage."[101] Microsoft appealed the district court's decision, stating the government seeks an impermissible extraterritorial application of the Electronic Communications Privacy Act (ECPA)[102] and the Second Circuit agreed, stating that warrant was invalid because of territoriality concerns.[103]

---

[96] 18 U.S.C. § 2518(5) (1976).

[97] Weinstein et al., *supra* note 87, at 750.

[98] *Id*.

[99] *Id*.

[100] *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624, at *1 (S.D.N.Y. Aug. 29, 2014).

[101] *Id*. at *4.

[102] In the Matter of A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION, Microsoft Corporation, Appellant, v. United States of America, Appellee., 2015 WL 1754413 (2d Cir.), 3-4 (Apr. 8, 2015).

[103] In the Matter of A Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 201 (2d Cir. 2016).

¶44 Even more recently, since the early drafts of this comment, this issue received a lot of media coverage in the government's case against Apple to decrypt the phone of one of the San Bernardino shooters. Like Microsoft, Apple is attempting to enforce the rights of its users against the government's security concerns. The F.B.I asked Apple to help unlock the iPhone of one of the shooters who killed 14 people in San Bernardino, California, Syed Rizwan Farook.[104] Apple refused, which prompted the F.B.I to try to get a court order to make Apple comply.[105] A magistrate judge granted the order, requiring Apple to aid the government to help bypass the auto-erase function if it was enabled, to allow the government to try passcodes on the device without permanently locking and without the additional delay usually in place on iPhones.[106] Apple responded with a letter to their customers that they plan to fight the order, stating that encryption helps the security of personal information, which ultimately helps personal safety.[107] Apple stated that the F.B.I wanted them to build a backdoor and Apple warned that once this was created, there would be no way to control its use – once the decryption key was created, it could be used on any device.[108]

¶45 The courts have two options if they treat encrypted messages analogously to former case law. They can either treat messages as a locked box (expectation of privacy) or like a secret or coded communication (no expectation).[109] They may also create a new understanding instead of trying to force the technology onto older law.[110] One hopes this would be the outcome, as technology may not overlay perfectly with the more tangible world the court hopes to compare it with.

B. Recommendations

¶46 Privacy should be weighed more heavily, especially when the only solutions at the moment seem to be to either turn over entire email accounts or to turn over nothing at all. At the risk of losing evidence, privacy should be the dominant concern, which has been supported by the Supreme Court noting that "privacy comes at a cost".[111] There is no need to expose all of one's private and personal thoughts in email. Law enforcement currently is required to stop listening on a wiretap when a conversation is irrelevant to their investigation.[112] Therefore, there is already a chance that law enforcement may be missing pertinent information to their investigations.

---

[104] Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gnman's iPhone,* N. Y. TIMES, Feb 17, 2016 http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0 [https://perma.cc/MKV5-ZEDP].

[105] *Id.*

[106] *In re* An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543, at *2 (C.D. Cal. Feb. 16, 2016)

[107] Apple, *A Message to Our Customers*, Feb. 16, 2016,http://www.apple.com/customer-letter/ [https://perma.cc/XA8F-8ZLC].

[108] *Id.*

[109] Emma Raviv, *Homing In: Technology's Place in Fourth Amendment Jurisprudence*, 28 HARV. J. L. & TECH. 593, 614 (2015).

[110] *Id*.

[111] Riley, 134 S. Ct., at 2493.

[112] *See* 18 U.S.C. § 2518(5) (1976).

¶47 Law enforcement says encryption could keep them from uncovering a terrorist plot, or prevent them from finding the organizers of domestic terrorism in the San Bernardino Case. They cite to security concerns as the reason for their desire to get technology companies to cooperate. However, there is another security interest that encryption helps, rather than hinders: digital security. Encryption keeps people's communications and information private, thereby preventing hacking and other digital security risks. Opening up the digital system to law enforcement is likely to open the system up to outside hackers, interested in stealing people's information and causing more crime even as law enforcement tries to prevent it. Apple has cited to this exact reason in their response to government pleas to decrypt the San Bernardino phone, highlighting industry fears.[113]

¶48 Law enforcement was previously able to get information on suspects, when wiretaps had to be installed manually and officers had to physically be on surveillance.[114] Law enforcement can get court permission to enter a home and plant a bug.[115] This requires more manpower than a typical wiretap, which can be accessed by a phone call to a telecommunications company, but it also defeats any law enforcement argument that without allowing wiretapping and warrants for encrypted information, the public will be in danger.[116] The court has preferred surveillance methods that uphold the Fourth Amendment to those that are convenient.[117]

¶49 Some scholars have warned against ubiquitous encryption as a way to protect privacy interests and deal with gaps in the statutory law, because it would force law enforcement to use alternatives to wiretaps and warrants to gain the information such as spyware installed on suspects' computers, or electromagnetic surveillance.[118] However, this argument, while valid, is not correct. The move should be towards further encryption, and further user protections. As this paper has shown, the statutory protections for communications are outdated, and case law is divided across the county, without a real trend emerging. Edward Snowden's disclosures revealed the government is already using illegal methods to discover information. Therefore, until the law becomes more settled and modern, the best way to protect the user is to increase encryption and make it a default setting. That will prevent companies from being able to send the information to law enforcement, because they will be unable to get access themselves.

¶50 Admittedly, this will make digital surveillance more difficult, and thereby more difficult for law enforcement to catch criminals, even including the terrorists often cited

---

[113] In re *An Apple iPhone*, 2016 U.S. Dist. LEXIS 20543, at *2.

[114] Christopher Soghoian, *Privacy and Law Enforcement: Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 399 (2010).

[115] *Id.*

[116] *Id.*

[117] *See* Berger v. New York, 388 U.S. 41, 62-63, (1967) ("In any event we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement. . . . [I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that without the use of such devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and -- what is more important -- without attending illegality.").

[118] Singleton, *supra* note 42, at 318, 320.

to in anti-privacy arguments. However, there are methods of surveillance that do not involve complete access to written communications. There are methods which may require more manpower, such as tailing or actual installation of recording equipment in a home. Because these methods are obviously invasive, rather than subtly so, like wiretapping or warrants for accounts or phones, and there is more case law on the right of privacy in these types of surveillance, people's right to privacy will be better protected. For now, an open invitation to gain access to a person's private thoughts and other data is not acceptable, even at the risk of the decreased ability of law enforcement to have access to information.

CONCLUSION

¶51 At the moment, privacy rights have the benefit of technology behind them. Many communications are very difficult for law enforcement to investigate, especially in a live feed via wiretapping, but also through warrants, as encrypted communications make it increasingly difficult for companies to comply with warrants for their users' account information.