THE YALE LAW JOURNAL

COMMENT

Law Enforcement and Data Privacy: A Forward-Looking Approach

The Edward Snowden revelations illustrated the ramifications of a domestic and international legal infrastructure that failed to keep up with technological advancements. The USA PATRIOT Act and other national security laws were ill-equipped to handle developments in bulk data collection. This failure is increasingly evident in the law enforcement context as well. Cloud computing and encryption have fundamentally unsettled the assumptions underlying the existing warrant regime.

The privacy concerns that crystallized in the wake of the Snowden disclosures have had ripple effects beyond the national security context. Private companies, NGOs, and foreign governments reacted forcefully to the revelations, effecting new laws and policies to shield information from the National Security Agency. A defining feature of this new era is the increasingly contentious relationship between the U.S. government and major U.S. technology companies, such as Apple and Google.[1] Foreign customers, suspicious of U.S. technology companies' relationship with the government, have threatened to switch to local Internet providers. The commercial implications of such a switch would be severe. By some estimates, losing business abroad could cost U.S. technology companies over one hundred

1. *See, e.g.*, Matt Apuzzo et al., *Apple and Other 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 [http://perma.cc/SQL9-WHLL]; Cory Bennett, *Apple Couldn't Comply with Warrant Because of Encryption*, HILL (Sept. 8, 2015), http://thehill.com/policy/cybersecurity/252896-apple-rebuffed-warrant-because-of-encryption [http://perma.cc/9YLP-7F72]; Michael B. Farrell, *FBI, DOJ Want Tech Industry To Find Workaround to 'Warrant-Proof' Encryption*, CHRISTIAN SCI. MONITOR (Sept. 15, 2015), http://www.csmonitor.com/World/Passcode/2015/0915/FBI-DOJ-want-tech-industry-to-find-workaround-to-warrant-proof-encryption [http://perma.cc/9HXM-EJP7].

eighty billion dollars in the market for cloud computing.[2] Accordingly, these companies have abandoned their longstanding policies of quiet cooperation with Washington. Instead, they now seek to outdo one another in demonstrating their independence from the government and their commitment to consumer privacy. For instance, Microsoft, with the support of many others in the industry, is in the midst of litigation challenging the territorial scope of U.S. warrants.[3] Apple and Google recently announced that their new systems would encrypt content on mobile phones in a manner that makes it impossible for the companies themselves to access the data on locked phones.[4] By encrypting content so heavily as to render warrants ineffective, this policy poses a direct obstacle to law enforcement's ability to access necessary electronic content.

In conjunction with new technologies that make such noncompliance possible, this acrimony clarifies the need to update the existing warrant doctrine. This Comment aims to begin that process. It rethinks the reach of warrants in light of cloud computing and proposes a legislative mechanism to ensure the continued effectiveness of warrants given developments in encryption technology. In doing so, this Comment strives to introduce better incentives and align the numerous interests implicated in data regulation. In order to succeed in the long run, any successful warrant regime must account for not only the government's interest in law enforcement, but also the individual consumer's interest in privacy and the commercial interests of technology companies.

Part I surveys the problems that recent developments have exposed in the current legal regime. Part II argues that in an era of cloud computing, hinging law enforcement access to data on its physical location increasingly makes little sense. Part III explores how encryption renders even clearly valid warrants insufficient and recommends legislative reform to address this impending reality.

2. Claire Cain Miller, *Google Pushes Back Against Data Localization*, N.Y. TIMES: BITS (Jan. 24, 2014, 6:28 PM), http://bits.blogs.nytimes.com/2014/01/24/google-pushes-back-against-data-localization [http://perma.cc/N9DK-6A76].

3. Dominic Rushe, *Tech Companies Join Microsoft in Email Warrant Case Against US Government*, GUARDIAN (Dec. 15, 2014), http://www.theguardian.com/technology/2014/dec/15/microsoft-email-warrant-lawsuit-tech-media-companies-join [http://perma.cc/5WXU-6CXB]; Alex Ely, *Second Circuit Argument in the Microsoft-Ireland Case: An Overview*, LAWFARE (Sept. 10, 2015, 5:08 PM), http://www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview [http://perma.cc/CQ3H-MQ3M].

4. *See infra* text accompanying note 40.

I. LAW ENFORCEMENT AND PRIVACY: THE ECPA'S OUTDATED APPROACH

Since 1986, the Electronic Communications Privacy Act (ECPA) has regulated law enforcement's ability to access electronic data. Its second section, the Stored Communications Act (SCA), stipulates that providers must disclose the content of electronic communications held in an account for more than 180 days if the government produces a subpoena or court order.[5] If such communication has been stored for fewer than 180 days, the government must obtain a search warrant.[6] Whereas the Fourth Amendment "probable cause" standard is required for a warrant, the government can obtain a subpoena or court order if it can establish reasonable grounds to believe that the contents are relevant to a criminal investigation—a lower standard.[7] As is readily apparent, the ECPA is sorely outdated in terms of the kinds and scope of privacy protection it offers. The distinctions drawn in the ECPA between communications stored for more or less than 180 days are vestiges of a bygone era, and many have argued that they should be abolished.[8] Yet as a recent Second Circuit case illustrates, the ECPA's problems go deeper than these artificial lines.

In December 2013, federal prosecutors obtained a warrant for emails associated with an account held by Microsoft. Because much of the email content was stored on servers in Ireland, Microsoft challenged the warrant, arguing that it could not be applied extraterritorially. Microsoft pointed to the Federal Rules of Criminal Procedure as well as the statutory presumption against extraterritoriality.[9] It argued that in order to obtain the email content, the United States must go through the bilateral process established in the Mutual Legal Assistance Treaty (MLAT) between the United States and

5. 18 U.S.C. § 2703(a), (b) (2012); *see* CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 41 (2012).

6. 18 U.S.C. § 2703(a).

7. *See* Griffin v. Wisconsin, 483 U.S. 868 (1987).

8. *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 66 (2014), http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf [http://perma.cc/WC4L-GRWR] (recommending that the ECPA's "archaic distinctions between email left unread or over a certain age" be revised so as to better track protections accorded to content in the physical world).

9. *In re* Warrant To Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014), *argued*, No. 14-2985-CV (2d Cir. Sept. 9, 2015).

Ireland.[10] Under that mechanism, Irish courts would determine the validity of the request pursuant to their own local law before turning over data to U.S. authorities—a notoriously slow and cumbersome process.[11] Yet in *In re Warrant To Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, the court rejected this argument, declaring that, under the SCA, U.S. Internet service providers served with a warrant must produce information "within [their] control" regardless of where it is stored.[12] Microsoft appealed, and a decision from the Second Circuit is expected in the coming months.[13]

Regardless of the outcome, the case highlights the limitations of the SCA, particularly the uncertainty about its extraterritorial application and scope. The statute was devised for a world in which the Internet was predominantly an American system. Yet in the past decades, the Internet has become thoroughly global, both in terms of its users and infrastructure. The SCA has failed to keep up with this transformation. In response, a bipartisan group of senators has attempted to address this deficiency by proposing the Law Enforcement Access to Data Stored Abroad Act (LEADS Act).[14] The LEADS Act requires a warrant for any access to communications content[15] and stipulates that warrants served

10. *Id.* at 474. MLATs are agreements between countries that have the status of international law and allow governments to exchange evidence and information with other jurisdictions in order to facilitate criminal investigations and prosecutions. *See* Drew Mitnick, *The Urgent Need for MLAT Reform*, ACCESS BLOG (Sept. 12, 2014, 4:42 PM), http://www.accessnow.org/blog/2014/09/12/the-urgent-needs-for-mlat-reform [http://perma.cc/6M7K-QWKL]. The United States has entered into over sixty MLATs. *See* Bureau of Int'l Narcotics & Law Enf't Affairs, *2012 INCSR: Treaties & Agreements*, U.S. DEP'T ST. (Mar. 7, 2012), http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm [http://perma.cc/B9AP-X3H7].

11. The White House estimates it takes ten months for MLAT requests to be fulfilled; others put the number much higher. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY & SECURITY IN A CHANGING WORLD 227 (2013) [hereinafter LIBERTY & SECURITY IN A CHANGING WORLD].

12. *In re Warrant*, 15 F. Supp. 3d at 474.

13. *See* Joe Palazzolo, *Microsoft Email Case Tests Power of Search Warrants*, WALL ST. J. (Sept. 7, 2015), http://www.wsj.com/articles/microsoft-email-case-tests-power-of-search-warrant-1441660355 [http://perma.cc/UM48-3GKC].

14. S. 512, 114th Cong. (2015); *see* Nancy Scola, *Senate's New Overseas-Email Protection Act Gets Mixed Reviews*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/senates-new-overseas-email-protection-act-gets-mixed-reviews [http://perma.cc/S9T5-PZ7L].

15. This requirement follows from the Sixth Circuit's ruling in *United States v. Warshak*, in which the court reasoned that, because "email is analogous to a letter or a phone call," individuals "enjoy[] a reasonable expectation of privacy in the content of emails 'that are stored with, or sent or received through, a commercial ISP.'" 631 F.3d 266, 286-88 (6th Cir. 2010). *Warshak*, in conjunction with pressure from civil society, played a crucial role in ensuring that the warrant requirement made it into reform proposals introduced in subsequent years, such as the LEADS Act.

to U.S. providers cover content stored abroad (as well as content stored in the United States) if that content is held in the account of a U.S. person. For non-U.S. persons whose content is stored abroad, the government must go through the MLAT system.[16] While the bill marks an important first step, a closer look reveals that it does not fully address the flaws of the SCA.

II. RETHINKING THE REACH OF WARRANTS IN THE ERA OF THE CLOUD

The approach embodied by current proposals for reform, such as the LEADS Act, is insufficient in an era of rapidly changing technology—in particular, cloud computing. The Act's limitations reveal the need to adjust the current focus on territoriality. A warrant regime that hinges on user nationality and content origination preserves law enforcement's ability to investigate effectively by securing a warrant of appropriate scope, but creates better incentives than the current territorial approach and is more attuned to the commercial and privacy interests at stake.

A. The Weaknesses of the LEADS Approach

Most problematically, the LEADS approach will be unable to keep pace with advancements in cloud computing. In cloud computing, Internet service providers move data among different data servers all over the world, rather than storing data in one physical location. This design is meant to meet users' needs efficiently and balance burdens on the networks used by providers. Its benefits are purported to include significant cost savings as well as increased innovation,[17] and the market for such services is expected to be two hundred seven billion dollars annually by 2016.[18] Yet if the premise of cloud computing is a load-balancing system that stores data in different countries at different points in time, the LEADS Act approach leaves critical questions unanswered when content belongs to non-U.S. persons. How are we to discern whether a U.S. warrant can reach the data? Will a U.S. warrant be applicable if the data was *ever* stored in the United States? Or is it valid only *while* the data is stored

16. S. REP. NO. 113-34, at 4 (2013); *see also* LIBERTY & SECURITY IN A CHANGING WORLD, *supra* note 11, at 226.

17. Louis Columbus, *Making Cloud Computing Pay*, FORBES TECH. (Apr. 10, 2013, 8:01 PM), http://www.forbes.com/sites/louiscolumbus/2013/04/10/making-cloud-computing-pay-2 [http://perma.cc/K3HA-CKQC]; Quentin Hardy, *Computing Goes to the Cloud. So Does Crime*, N.Y. TIMES: BITS (Dec. 2, 2014, 9:10 PM), http://bits.blogs.nytimes.com/2014/12/02/computing-goes-to-the-cloud-so-does-crime [http://perma.cc/28DC-9DFN].

18. LIBERTY & SECURITY IN A CHANGING WORLD, *supra* note 11, at 211.

in the United States? This ambiguity constitutes a critical shortcoming that will become more acute as the Internet grows more cloud-centered.

Relatedly, when government access to information turns on the physical location of servers, it increases pressure for data localization mandates. Data localization laws require companies to store data collected in a country on servers in that country. Technology companies have vehemently protested such mandates, emphasizing that localization does not make data more secure and that it could result in the "effective Balkanization of the Internet and the creation of a 'splinternet' broken up into smaller national and regional pieces . . . to replace the global Internet."[19] Nonetheless, in the post-Snowden era, many foreign governments have proposed or passed such laws in a purported effort to protect their citizens from U.S. surveillance.[20] The dichotomy set up by the LEADS Act approach will accelerate this trend. It gives credence to the notion that governments have special ownership over data stored physically within their borders. In doing so, it encourages foreign governments to view localization mandates as a mechanism for avoiding time-consuming and uncertain requests to other countries when their law enforcement requires access to electronic content.

The impact of this trend is significant. Data localization would severely threaten the development and use of cloud computing. Forcing companies to store data on particular servers prevents them from rotating data most efficiently among servers. Localization would also result in companies inefficiently building servers in a country that may have high energy costs or

19. Miller, *supra* note 2.

20. *See, e.g.*, Allison Grande, *Apple's China Data Storage Portends Localization Movement*, LAW360 (Aug. 22, 2014, 5:52 PM), http://www.law360.com/articles/569841/apple-s-china-data-storage-portends-localization-movement [http://perma.cc/E35N-UMVA] (China); Allison Grande, *Brazil Nixes Data Localization Mandate from Internet Bill*, LAW360 (Mar. 20, 2014, 5:19 PM), http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill [http://perma.cc/37DN-6E26] (Brazil); Natalia Gulyaeva et al., *Russia Changes Effective Date of Data Localization Law to September 2015*, HOGAN LOVELLS CHRON. DATA PROTECTION (Jan. 2, 2015), http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/russia-changes-effective-date-of-data-localization-law-to-september-2015 [http://perma.cc/LFL6-2PQ4] (Russia). While many of these mandates seem to be motivated by governments' desire to increase their own scrutiny of Internet activity, even France and Germany have proposed the creation of a European Internet. *See Germany, France To Mastermind European Data Network–Bypassing US*, REUTERS (Feb. 16, 2014), http://www.rt.com/news/european-data-protection-network-283 [http://perma.cc/3E5T-CJKB]; Alexander Plaum, *The Impact of Forced Data Localisation on Fundamental Rights*, ACCESS BLOG (June 4, 2014, 9:01 AM), http://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights [http://perma.cc/V8H6-EP3T].

inadequately trained engineers.[21] Moreover, it would divide the Internet into fragmented, national domains, rather than the global commons it has operated as thus far.[22] Lastly, localization would make data less secure. By pooling and storing data in designated physical sites, it creates easy targets for hackers. One of the virtues of the cloud is that it replaces this static data pooling with a more dynamic system of storage that is tougher to penetrate.[23]

An additional drawback of the LEADS Act dichotomy is that it creates incentives for lawbreakers to shift information to the accounts of non-U.S. persons to avoid process. It is conversely *more* privacy-protective of non-U.S. persons than U.S. persons: when data is stored abroad, the former's accounts are effectively shielded from U.S. law enforcement access but the latter's are not, even though the individuals may be engaged in the same illicit activity alongside one another. Given the uncertainty and delays of the MLAT process, this two-tier system is likely to produce attempts to evade the reach of warrants by transferring criminal information, such as stolen credit card numbers, to non-U.S. persons. This approach is also at odds with existing Fourth Amendment doctrine, which generally requires *heightened* constitutional protection for U.S. citizens.[24]

Lastly, reciprocal application of the LEADS Act framework would be problematic. If foreign governments adopted the U.S. approach, they could assert extraterritorial authority over communications by their own citizens that are stored in the United States. This approach is in tension with the current procedure, whereby foreign governments requesting data stored in the United States by U.S. providers must go through the MLAT process.[25] Moreover, it is unclear what process foreign governments must go through to request their own citizens' data from *foreign* providers who *happen* to store their data in the

21. Bob Butler et al., *Cloud Computing Under Siege*, FCW (Sept. 12, 2014), http://fcw.com/articles/2014/09/12/cloud-under-siege.aspx [http://perma.cc/QP36-XZPU].

22. *See* Michael Chertoff, *The Strategic Significance of the Internet Commons*, STRATEGIC STUD. Q., Summer 2014, at 10.

23. Experts also maintain that the cloud is more secure than traditional platforms because data security hinges not on the location of data, but on elite cybersecurity talent and comprehensive security protocols, which companies offering sophisticated cloud services, such as Google and Amazon, are better able to provide. *See* Robb Allen, *Why the Cloud Can Be More Secure than Your Private Network*, DATAPIPE (Mar. 17, 2014), http://www.datapipe.com/blog/2014/03/17/why-the-cloud-can-be-more-secure-than-your-private-network [http://perma.cc/68W5-S8RR]; Hardy, *supra* note 17.

24. *Compare* United States v. Verdugo-Urquidez, 494 U.S. 259, 270 (1990) (holding that a defendant could not invoke the fourth amendment for conduct abroad because he was not a U.S. citizen), *with* Reid v. Covert, 354 U.S. 1, 33 (1957) (holding that U.S. citizens stationed abroad were protected by the fifth and sixth amendments).

25. LIBERTY & SECURITY IN A CHANGING WORLD, *supra* note 11, at 226–27.

United States. These issues reveal the deeper problem with the privacy regime in place under the ECPA and as envisioned by the LEADS Act. Conditioning access to electronic communications on where the data is stored makes little sense in the era of the cloud. The physical location of data, which could change at different points in time, is the product of a fairly random technical decision. While territoriality remains an important variable, the current focus on where information is stored is misplaced.

B. Reorienting the Focus on Territoriality

In considering territoriality, a more forward-looking approach should focus on where the user resides and where content is produced. Under such a framework, the degree of protection accorded to particular electronic content by the United States would hinge on the nationality of the user and the location where the content originated—thereby eliminating existing incentives for localization that dampen progress in cloud computing. U.S. warrants would be sufficient to require companies to produce requested data regardless of where it is stored, provided either that the data belongs to a U.S. person or that the user activity originates in the United States.[26] In contrast, the government would have to go through the MLAT process to access data pertaining to non-U.S. nationals that originated abroad. Moreover, the United States should *allow* Internet providers to produce content stored in the United States pursuant to foreign legal process, if such content belongs to the nationals of that country or if the user activity took place there.[27] Companies could opt out of compliance with foreign court orders if they chose, but the United States should not *require* that foreign governments go through the MLAT process and obtain permission under U.S. law, simply because data otherwise entirely unconnected to the United States happens to be stored there.

Turning the focus from territoriality—the physical location of the data—to the nationality of the user and the location of the relevant conduct would track traditional fault lines in Fourth Amendment law. Namely, U.S. persons continue to be protected by the Fourth Amendment even when traveling

26. This stands in contrast to other scholars, who have argued for abandoning territoriality, *see* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE. L.J. 326 (2015), or for preserving territorial distinctions along different metrics, *see* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014).

27. Currently, foreign governments requesting data stored in the United States by U.S. providers must go through the MLAT process. LIBERTY & SECURITY IN A CHANGING WORLD, *supra* note 11, at 226-27.

abroad,[28] but non-U.S. persons outside U.S. territory do not enjoy such protections.[29] This approach would better reflect the underlying *reasons* for according certain individuals or activities privacy rights vis-à-vis the U.S. government: the individuals are members of a community safeguarded from such intrusions by its government, or their actions enjoy an expectation of privacy by virtue of their physical presence in the United States.

Similarly, limiting the scope of warrants in this manner would comport with foundational principles of international law, particularly respect for state sovereignty and comity. These principles underlie the longstanding prohibition on using law enforcement capabilities in another state's territory.[30] They prevent the United States from exercising its police power abroad, even when it has the capacity to do so. In accordance with these principles, U.S. law enforcement is forced to rely on mechanisms such as legal assistance treaties and letters rogatory when relevant evidence or persons are outside U.S. territory.[31] U.S. law enforcement should be similarly compelled to go through the MLAT process in order to obtain data belonging to foreign citizens that originates abroad. This framework would acknowledge that other countries have a far greater interest in the content of such data, since it pertains to their nationals or was created on their territory. Just as the United States would not want a foreign government, which may be far less protective of individual privacy, to be able to obtain content produced by U.S. nationals on U.S. soil just because such data happens to be stored on servers abroad, it should refrain from accessing data produced abroad by foreign nationals simply because it happens to be stored on U.S. servers. In the long term, then, the principles of comity and respect for state sovereignty, which compel the United States to

28. *See, e.g.*, *Verdugo-Urquidez*, 494 U.S. at 270 (distinguishing *Reid v. Covert* on the ground that the defendant seeking to invoke the Fourth Amendment in this case was not a U.S. citizen); United States v. Conroy, 589 F.2d 1258, 1264 (5th Cir. 1979) ("The Fourth Amendment not only protects all within our bounds; it also shelters our citizens wherever they may be in the world from unreasonable searches by our own government.").

29. *Verdugo-Urquidez*, 494 U.S. at 274-75 (holding that "the Fourth Amendment has no application" to the search by U.S. agents of property owned by a Mexican citizen and located in Mexico).

30. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW §§ 401-04, 432 (AM. LAW INST. 1987). The Permanent Court of International Justice in *S.S. Lotus*, a seminal international law case, stated that "the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State." S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

31. CHARLES DOYLE, CONG. RESEARCH SERV., RL94-166, EXTRATERRITORIAL APPLICATION OF AMERICAN CRIMINAL LAW 22-25 (2012).

limit the reach of its warrants in the manner described, also provide greater protection to U.S. nationals.

This approach is admittedly imperfect. For one, lingering challenges would remain for those accounts that could not be traced or identified, such as anonymized IP addresses. However, Internet geolocation technology, which aims to pinpoint the physical location of Internet users or devices, has grown increasingly sophisticated in recent years.[32] Internet providers use IP-address-based geolocation techniques in conjunction with others, such as collecting the time it takes for a device to respond to pings or analyzing the manner in which it routes information, which has improved accuracy.[33] While extremely savvy users could potentially still avoid being traced, recent developments have made avoiding detection far more technologically challenging.[34] Consequently, there is a low likelihood that a datastream would be so obscured that Internet providers could not provide a rough estimate as to its origins.

Another potential problem with this approach is that reciprocal application could result in the disclosure of sensitive communications to hostile governments, without the protections of the U.S. judicial process.[35] Yet in the long term, requiring countries to go through the U.S. legal process when data is stored in the United States, even though they may have a far greater interest in the content, is counterproductive. Reciprocal application of this requirement entrenches an outdated notion of territoriality that could leave U.S. citizens' user data vulnerable to information requests from less-protective regimes. It also increases the pressure for localization mandates and threatens the development of the cloud, which offers more security than traditional computing.[36] Preserving the current approach would therefore make data *less* secure. Moreover, the concern with reciprocal application will be increasingly less salient as cloud computing grows and data rotates among servers around the world. It is also important to bear in mind that the United States already has legal assistance agreements with countries such as Russia and China,

32. *See* Riva Richmond, *We Know Where You Are*, WALL ST. J. (Sept. 29, 2008), http://www.wsj.com/articles/SB122227759888771725 [http://perma.cc/S7QW-ZZ5V].

33. James A. Muir & Paul C. van Oorschot, *Internet Geolocation: Evasion and Counterevasion*, ACM COMPUTING SURVEYS, Dec. 2009, at 1, 8-10; *see* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 592-97 (2012).

34. *See* Muir & van Oorschot, *supra* note 33, at 1; Jamie Taylor et al., *Bringing Location to IP Addresses with IP Geolocation*, 4 J. EMERGING TECHNOLOGIES WEB INTELLIGENCE 273 (2012).

35. The paradigmatic example of this undesirable situation is an illiberal regime requesting data belonging to a human rights activist from that country, in which the user activity originated abroad but the data happens to be stored on servers in the United States.

36. *See supra* note 23 and accompanying text.

pursuant to which it frequently exchanges information and evidence in the nonelectronic context.[37] The vast majority of this cooperation involves run-of-the-mill investigations, in which such exchange is mutually beneficial and poses little concern—as is likely to be the case in the electronic context as well.[38]

In short, the existing legal regime governing the reach of warrants was not designed with technological innovations such as the cloud in mind. Rather, it creates undesirable incentives for a "splinternet." Shifting the focus to the nationality of the user and where the content originates would better prepare the legal framework to accommodate further developments in cloud computing. Further, this approach would strike a balance between law enforcement and privacy that both tracks the Fourth Amendment's protections and comports with international law.

III. ENCRYPTION: WHEN WARRANTS ARE NOT ENOUGH

Updating U.S. legal infrastructure to keep up with new technologies does not end with revising the ECPA. A clearly valid warrant is no longer sufficient for law enforcement to obtain requested data. In order to ensure the effectiveness of the warrant regime, then, legislation should compel companies to maintain decryption capabilities but impose stricter minimization requirements.

A. Trending Toward Noncooperation

As the relationship between Washington and major U.S. technology companies has grown more contentious, companies have not only declined to cooperate with the government unless mandated by a court order, but they have also accelerated efforts to more heavily encrypt data—both when it is

37. *See* Agreement on Mutual Legal Assistance in Criminal Matters, China-U.S., June 19, 2000, T.I.A.S. No. 13,102; Treaty on Mutual Legal Assistance in Criminal Matters, Russ.-U.S., June 17, 1999, S. TREATY DOC. NO. 106-22; *see also* BRUCE ZAGARIS, INTERNATIONAL WHITE COLLAR CRIME: CASES AND MATERIALS 275-93 (2010); Anna MacCormack, *The United States, China, and Extradition: Ready for the Next Step?*, 12 N.Y.U. J. LEGIS. & PUB. POL'Y 445 (2012).

38. *See, e.g.*, BUREAU OF INT'L NARCOTICS & LAW ENF'T, U.S. DEP'T OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT 197 (2010), http://www.state.gov/documents/organization/137411.pdf [http://perma.cc/M68N-UE28] (describing U.S.-China cooperation to combat drug trafficking); Duncan DeVille, *Prosecuting Russian Organized Crime Cases*, 3 CHI. J. INT'L L. 493 (2002).

stored in servers and as it moves among them.[39] In general, the U.S. government should welcome this development. Encrypting electronic communications makes data more secure, making it harder for hackers and cybercriminals to infiltrate. Yet technology companies have gone further. In September 2014, Apple and Google announced that their new systems would encrypt content on mobile phones in a manner that makes it impossible for the companies themselves to access the data on locked phones.[40] Facebook and WhatsApp followed with similar announcements, spurring investment in companies promising even more sophisticated end-to-end encryption.[41]

The implications for law enforcement are significant. Under Apple's iOS 8 mobile operating system, for instance, data on iPhones is by default encrypted once users set a passcode. Once this is done, Apple is technologically unable to access the encrypted data, even when served with a warrant. In prior systems, by contrast, law enforcement officials with court orders could send iPhones to Apple's headquarters for engineers to recover the requested data.[42] Under the new systems, data that is backed up on iCloud servers and retained by third parties, such as call logs, would still be accessible to law enforcement.[43] Yet it is not difficult to imagine that a few years down the road, such stored data will soon be encrypted in this manner as well.

The possibility of decreasing access to data, particularly data that an Article III court has determined with probable cause contains evidence of a crime, has engendered strong criticism from the law enforcement community.[44] High-

39. David E. Sanger & Nicole Perlroth, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. TIMES (June 6, 2014), http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html [http://perma.cc/XWG2-BA3V].

40. Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, WALL ST. J. (Sept. 22, 2014), http://www.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341 [http://perma.cc/M4DN-VCCP].

41. Tom Fox-Brewster, *WhatsApp Adds End to End Encryption Using TextSecure*, GUARDIAN (Nov. 19, 2014), http://www.theguardian.com/technology/2014/nov/19/whatsapp-messaging-encryption-android-ios [http://perma.cc/BP6Q-QN8U]; Amrita Jayakumar, *Encryption Company Silent Circle, Creator of Blackphone, Raises $30 Million*, WASH. POST (May 21, 2014), http://www.washingtonpost.com/business/capitalbusiness/encryption-company-silent-circle-creator-of-blackphone-raises-30-million/2014/05/21/0f9f0820-e103-11e3-8dcc-d6b7fede081a_story.html [http://perma.cc/639J-9N74]; Tom Risen, *Facebook Email Encryption Another Blow to Surveillance*, U.S. NEWS & WORLD REP. (June 2, 2015), http://www.usnews.com/news/articles/2015/06/02/facebook-email-encryption-another-blow-to-surveillance [http://perma.cc/QBX9-EVDT].

42. Barrett & Yadron, *supra* note 40.

43. *Id*.

44. *See* Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police out of Phones*, WASH. POST (Sept. 25, 2014), http://www.washingtonpost.com/business/technology/2014

level officials, including the President, have exerted significant pressure on companies to modify such systems;[45] yet technology companies have remained steadfast.[46]

In light of the growing standoff, there are several options available to the United States. First, the government can attempt to persuade companies to drop their use of inaccessible systems. Recent developments, however, indicate that reliance on informal methods of cooperation between the government and companies is no longer sufficient.[47] Alternatively, law enforcement could rely solely on compelled decryption, whereby an individual served with a court order can be compelled to enter the passcode for his or her smartphone or be prosecuted for contempt of court. This route, though, applies only to situations in which the relevant individual can be tracked down, and raises Fifth Amendment self-incrimination concerns.[48] Another option is to pass legislation that requires companies to retain decryption ability so as to be responsive to law enforcement requests, with noncompliant companies facing an escalating series of fines. In the long run, this option is likely to be the most efficacious.[49]

/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html [http://perma.cc/2QLD-EKE2]; Chris Strohm, *New York Prosecutor Calls for Law To Fight Apple Data Encryption*, BLOOMBERG (Jan. 6, 2015, 5:23 PM), http://www.bloomberg.com/news/articles/2015-01-06/new-york-prosecutor-calls-for-law-to-fight-apple-data-encryption [http://perma.cc/6HNF-SCH6].

45. Allison Grande, *Obama Bashes Plans To Block Police Access to User Data*, LAW360 (Jan. 16, 2015, 5:43 PM), http://www.law360.com/articles/612572/obama-bashes-plans-to-block-police-access-to-user-data [http://perma.cc/FF2K-QZDP].

46. Danny Yadron, *Google's Schmidt Fires Back over Encryption*, WALL ST. J. (Oct. 8, 2014), http://www.wsj.com/articles/googles-schmidt-says-encrypted-phones-wont-thwart-police-1412812180 [http://perma.cc/7W34-BH2H].

47. Del Quentin Wilber, *U.S. Seeks To Reverse Apple-Android Data-Locking Decision*, BLOOMBERG (Sept. 30, 2014, 12:00 AM), http://www.bloomberg.com/news/articles/2014-09-30/u-s-seeks-to-reverse-apple-android-data-locking-decision [http://perma.cc/LA8H-2HB8].

48. Hanni Fakhoury, *Fifth Amendment Prohibits Compelled Decryption, New EFF Brief Argues*, ELECTRONIC FRONTIER FOUND. (Oct. 30, 2013), https://www.eff.org/deeplinks/2013/10/new-eff-amicus-brief-argues-fifth-amendment-prohibits-compelled-decryption [http://perma.cc/7ED6-XNCX] (arguing that law enforcement cannot force a crime suspect to decrypt his computer because doing so violates the fifth amendment privilege against self-incrimination).

49. Such a response would be in accord with the response of other countries, such as the United Kingdom. Chloe Albanesius, *U.K. Prime Minister Wants To Ban Encrypted Messaging*, PC MAG. (Jan. 13, 2015, 10:25 AM), http://www.pcmag.com/article2/0,2817,2475069,00.asp [http://perma.cc/5U4W-3SLL].

B. Possibilities for Legislative Reform

As the cloud and peer-to-peer communications platforms become more heavily trafficked and more vulnerable to criminal activity,[50] accessing data on such platforms will be increasingly critical to defeating criminal and terrorist activity. Currently, prosecution is the only recourse for the government when confronting recalcitrant technology companies. The government is often understandably reluctant to pursue this option, so as not to jeopardize cooperation in other domains and for fear of collateral consequences. Therefore, legislation that requires Internet providers to retain the ability to decrypt communications when served with warrants and imposes fines for failure to do so would be a less severe mechanism to engender cooperation. At the same time, the penalties would give teeth to the government's current entreaties, which are increasingly ignored.

Undoubtedly, any such legislation will face resistance from technology companies and NGOs, who will likely denounce it as an effort by the U.S. government to obtain a "backdoor" to user communications.[51] Such allegations seem to be driven by the similarities between this proposed measure and the 1994 Communications Assistance for Law Enforcement Act (CALEA).[52] The Act requires that all phone companies design their systems to provide an opening for government wiretaps and was amended in 2005 to apply to broadband and certain Internet phone services. This same Act could be further amended to bring Internet service providers and certain social media sites within its purview, with a critical distinction. Unlike the 1994 Act, any effort to obtain law enforcement access to encrypted data does not and should not require a back door. Rather than forcing companies to build in openings that the government is aware of and can exploit, any legislation should allow technology companies to design systems in a way that maximizes data security, so long as they retain *their own* ability to decrypt when required by court order.

50. *See* Ellen Nakashima, *Proliferation of New Online Communications Services Poses Hurdles for Law Enforcement*, WASH. POST (July 26, 2014), http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html [http://perma.cc/AD8V-ZYNC]; Hardy, *supra* note 17.

51. *See, e.g.*, Allison Grande, *Wyden Again Floats Bill To Bar Backdoor Access to User Data*, LAW360 (Jan. 9, 2015, 5:38 PM), http://www.law360.com/articles/609913/wyden-again-floats-bill-to-bar-backdoor-access-to-user-data [http://perma.cc/RX9F-89TY]; Jake Laperruque, *Tales from Decrypt: FBI Wants Backdoors and Ability To Compel Access*, CTR. FOR DEMOCRACY & TECH. (Oct. 17, 2014), http://cdt.org/blog/tales-from-decrypt-fbi-wants-backdoors-and-ability-to-compel-access [http://perma.cc/3ZQA-6SY4].

52. 47 U.S.C. §§ 1001-1010 (2012) (amended 2005).

Even with the caveat that neither the United States nor any other government will possess a back door to access user content, such a proposal is sure to trigger some alarm. Yet the recent passage of the USA Freedom Act suggests that the political space and impetus exist to make enacting compromise reform measures of this kind possible.[53] Moreover, a carefully crafted statute could mitigate backlash. First, any legislative requirement of this kind should allow for a reasonable implementation period, perhaps twelve to twenty-four months. To be sure, requiring an opening in an encryption algorithm inevitably creates an entry point that can also potentially be exploited by nefarious actors.[54] (The other alternative, companies maintaining a "vault" of passwords that can later be accessed, has similar vulnerabilities.) However, allowing companies to develop opportunities for future interception when *designing* systems at the outset, rather than seeking to amend already-complete encryption algorithms to create an opening, would allow engineers to better secure such gaps.

Perhaps most importantly, any legislative reform, both with respect to the ECPA and encryption for law enforcement, should include strict minimization requirements.[55] The SCA includes no such limitations. Once the government serves Internet providers with a warrant for the communications content of a particular account, it is essentially free to sift through all of the available content in that account.[56] In contrast, when accessing communications from traditional phone companies under the CALEA, a government actor must tailor the search and screen communications and limit disclosure so that only relevant files are transferred to other agents.[57] Minimization would work differently in the electronic context than in the telephone context, but could be implemented just as effectively. Certain default metrics could be devised to trim the scope of access initially granted to government officials, based on factors such as the duration of communications, the time when the

53. *USA Freedom Act: What's in, What's out*, WASH. POST (June 2, 2015), http://www.washingtonpost.com/graphics/politics/usa-freedom-act [http://perma.cc/EJM5-67YJ].

54. *See* Nakashima, *supra* note 50.

55. Minimization requirements mandate that government officials implement procedures to limit the collection, retention, and dissemination of private information. These provisions can vary significantly in scope and detail. *See, e.g.*, 50 U.S.C. § 1801(h) (2012) (concerning minimization procedures under the Foreign Intelligence Surveillance Act). S*ee generally* 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 (1978).

56. *See* Kerr, *supra* note 26, at 384; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1701, 1723-24, 1739 (2004).

57. *See* Scott v. United States, 436 U.S. 128 (1978); United States v. McGuire, 307 F.3d 1192, 1202 (9th Cir. 2002).

communications were made, and the number of other actors involved. From there, an initial law enforcement official could perform discretionary filtering to screen content and pass along only that which meets a threshold of relevance, which could vary based on the severity of the crime or investigation in question. Together, these provisions would balance law enforcement's informational needs with users' privacy interests in a more nuanced manner.

Moreover, in spite of the inevitable initial backlash, such reforms are actually in the commercial interests of technology companies. Foreign customers have been suspicious of cooperation between U.S. companies and the government in part because their collaboration has been so furtive. By passing legislative reforms, the United States could make clear that the era of "secret cooperation" is over. Any disclosure by U.S. companies to the U.S. government will be the product of court orders, with the scope of such disclosure delineated by statute. This openness would arguably do more to assuage foreign and domestic consumer concerns than the acrimony of the past year.

The current trend in encryption has made securing a warrant insufficient for law enforcement to access electronic content. Legislation that requires companies to retain decryption ability, but institutes strict minimization requirements, is necessary to ensure the effectiveness of an updated warrant system, albeit in a manner that is sensitive to individual privacy and commercial interests.

CONCLUSION

Technological advancements, particularly the cloud and encryption, will soon render our current legal frameworks outdated. Preserving the balance between security and privacy in the context of law enforcement therefore requires updating our warrant regime to better align the incentives of government, technology companies, and individual consumers.

REEMA SHAH*

* Yale Law School, J.D. 2015. I am incredibly grateful to Jake Sullivan for teaching the course that inspired this Comment and advising the project. My deepest thanks to Professors Harold Koh, Amy Chua, and Paul Gewirtz for their generous feedback and support. Lastly, I am very grateful to Amanda Lynch, Dahlia Mignouna, Mike Clemente, and the editors of the *Yale Law Journal* for all of their wonderful suggestions and ideas—the piece has benefited tremendously from them.