PRIVACY AND SECURITY IN THE CLOUD: SOME REALISM ABOUT TECHNICAL SOLUTIONS TO TRANSNATIONAL SURVEILLANCE IN THE POST-SNOWDEN ERA

Joris V.J. van Hoboken and Ira S. Rubinstein

PRIVACY AND SECURITY IN THE CLOUD: SOME REALISM ABOUT TECHNICAL SOLUTIONS TO TRANSNATIONAL SURVEILLANCE IN THE POST-SNOWDEN ERA†

Joris V.J. van Hoboken and Ira S. Rubinstein***

I. INTRODUCTION

Since June 2013, the leak of thousands of classified documents regarding highly sensitive U.S. surveillance activities by former National Security Agency (NSA) contractor Edward Snowden has greatly intensified discussions of privacy, trust, and freedom in relation to the use of global computing and communication services. This is happening during a period of ongoing transition to cloud computing services by organizations, businesses, and individuals.[1] There has always been a question inherent in this transition: are cloud services sufficiently able to guarantee the security of their customers' data as well as the proper restrictions on access by third parties, including governments? While worries over government access to data in the cloud is a predominate part of the ongoing debate over the use of cloud services,[2] the Snowden revelations highlight that intelligence agency operations pose a unique threat to the ability of services to keep their

† The Authors would like to thank Claudia Diaz, Katherine Strandburg, Seda Gürses, Malte Ziewitz, Nathan Newman, Heather Patterson, Elana Zeide, and the editors of the Maine Law Review for their valuable feedback and contributions in various stages of writing this paper.

* Joris V.J. van Hoboken is a Microsoft Research Fellow at the Information Law Institute, New York University School of Law.

** Ira S. Rubinstein is a Senior Fellow at the Information Law Institute, and Adjunct Professor, New York University School of Law.

1. With respect to cloud services, we follow the accepted definition of cloud computing given by the National Institute for Standards and Technology (NIST): "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." PETER MELL & TIMOTHY GRANCE, NAT'L INST. FOR STANDARDS & TECH, U.S. DEP'T OF COMMERCE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2. *See, e.g.*, Fred H. Cate, James X. Dempsey, & Ira S. Rubinstein, *Systematic Government Access to Private-Sector Data*, 2 INT'L DATA PRIVACY L. 195, 198-99 (2012), *available at* http://idpl.oxfordjournals.org/content/2/4/195.full.pdf; Ira S. Rubinstein, Gregory T. Nojeim, & Ronald D. Lee, *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIVACY L. (forthcoming 2014), *available at* https://cdt.org/files/pdfs/govaccess2013/government-access-to-data-comparative-analysis.pdf; Joris van Hoboken, Axel Arnbak, & Nico van Eijk, *Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad* (June 7, 2013) (unpublished manuscript) (*available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103); Randal Milch, *Thoughts on Foreign Data Storage and the Patriot Act*, VERIZON POL'Y BLOG (Jan. 27, 2014), http://publicpolicy.verizon.com/blog/entry/thoughts-on-foreign-data-storage-and-the-patriot-act; Brad Smith, *Protecting Customer Data from Government Snooping*, OFFICIAL MICROSOFT BLOG (Dec. 4, 2013, 9:00 PM), http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx.

customers' data out of the hands of domestic as well as foreign governments.[3] The search for a proper response is ongoing, from the perspective of market players, governments, and civil society.

At the technical and organizational level, industry players are responding with the wider and more sophisticated deployment of encryption as well as a new emphasis on the use of privacy enhancing technologies and innovative architectures for securing their services.[4] These responses are the focus of this Article, which contributes to the discussion of transnational surveillance by looking at the interaction between the relevant legal frameworks on the one hand, and the possible technical and organizational responses of cloud service providers to such surveillance on the other. While the Article's aim is to contribute to the debate about government surveillance with respect to cloud services in particular, much of the discussion is relevant for Internet services more broadly.

A. Transnational Surveillance

Transnational surveillance of data in the cloud presents complex scenarios that are currently not handled in any satisfactory way by existing legal or technical mechanisms. Of particular complexity is the question of whether and how globally operating services can ensure that the data of an individual or organization in 'country T' (the targeted country) can be secured from disproportionate access by a government agency in 'country A' (the accessing country). In practice, many scenarios are even more complex, given there may be agencies in multiple countries seeking access to data of a particular organization, data that could be

---

3. *See infra* Parts I.B., III.

4. *See, e.g.*, Matthew Taylor, *NSA Revelations 'Changing How Businesses Store Sensitive Data'*, THE GUARDIAN, Mar. 31, 2014, http://www.theguardian.com/technology/2014/mar/31/data-storage-nsa-revelations-businesses-snowden; Nicole Perlroth, *A Call for a Highly Encrypted Future*, N.Y. TIMES BITS BLOG (Mar. 12, 2014, 6:56 PM), http://bits.blogs.nytimes.com/2014/03/12/a-call-for-a-highly-encrypted-future; Jon Fingas, *FreedomPop's New Smartphone Keeps Your Calls and Data Private for $189*, ENGADGET (Mar. 5, 2014, 12:00 AM), http://www.engadget.com/2014/03/05/freedompop-privacy-phone; Loek Essers, *KPN Strikes Deal with Silent Circle to Offer Encrypted Phone Calls*, PCWORLD (Feb. 19, 2014, 3:15 AM), http://www.pcworld.com/article/2099160/kpn-strikes-deal-with-silent-circle-to-offer-encrypted-phone-calls.html; David Meyer, *Meet Blackphone, A Privacy-Centric Handset from Some Serious Security Veterans*, GIGAOM (Jan. 15, 2014, 1:21 AM), http://gigaom.com/2014/01/15/meet-blackphone-a-security-centric-handset-from-some-serious-encryption-veterans; Nicole Perlroth & Vindu Goel, *Twitter Toughening Its Security to Thwart Government Snoops*, N.Y. TIMES BITS BLOG (Nov. 22, 2013, 4:22 PM), http://bits.blogs.nytimes.com/2013/11/22/twitter-toughening-its-security-to-thwart-government-snoops/?_php=true&_type=blogs&_r=0; Sean Gallagher, *Googlers say "F*** You" to NSA, Company Encrypts Internal Network*, ARS TECHNICA (Nov. 6, 2013, 3:35 PM), http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network; Claire Cain Miller, *Angry Over U.S. Surveillance, Tech Giants Bolster Defenses*, N.Y. TIMES, Nov. 1, 2013, at A1, *available at* http://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html; Kurt Opsahl, *6 Steps Silicon Valley Can Take to Protect Users from NSA Spying*, CNET (Oct. 30, 2013, 5:43 PM), http://news.cnet.com/8301-13578_3-57610139-38/6-steps-silicon-valley-can-take-to-protect-users-from-nsa-spying; Adrianne Jeffries, *Escape from PRISM: How Twitter Defies Government Data-Sharing*, THE VERGE (Jun. 13, 2013, 1:18 PM), http://www.theverge.com/2013/6/13/4426420/twitter-prism-alex-macgillivray-NSA-government. *See also* Smith, *supra* note 2.

stored and transmitted across multiple international locations.

It is well established that lawful access frameworks in different jurisdictions permit—to varying extents—transnational access to cloud data.[5] The use of transnational surveillance by foreign governments to access international data outside the terms of Mutual Legal Assistance Treaties is generally considered problematic from a legal perspective.[6] In Europe, the discussion has taken place with a particular reference to the USA PATRIOT Act and other U.S. lawful access authorities with possible extraterritorial effect.[7] Notably, research has shown that the extraterritorial application of such laws is not necessarily unique to the U.S.; rather, the U.S. occupies a unique position due to the global strength of U.S. cloud services.[8]

The question of transnational surveillance is of special interest for a number of reasons. First, it is likely that individuals, businesses, and organizations want to minimize foreign government access to their data.[9] Second, it has become clear that certain States may impose legal requirements on cloud services aimed at preventing such access from taking place. Examples of this include discussions about "localization" (i.e., requiring that services locate their operations inside the country where the service is offered and/or provide local storage of data) in Europe and Brazil, and the debate about the revision of the European data protection

---

5. *See, e.g.*, Rubinstein et al., *supra* note 2, at 43 (noting that "[a]s Internet-based services have become globalized, trans-border surveillance—surveillance in one country affecting citizens of another—has flourished").

6. *See, e.g.*, IAN BROWN & DOUWE KORFF, GLOBAL NETWORK INITIATIVE, DIGITAL FREEDOMS IN INTERNATIONAL LAW: PRACTICAL STEPS TO PROTECT HUMAN RIGHTS ONLINE (2012), *available at* http://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law_0.pdf.

7. *See, e.g.*, CASPAR BOWDEN, EUR. PARLIAMENT POL'Y DEPT., CITIZENS' RTS. & CONST. AFF., THE U.S. SURVEILLANCE PROGRAMMES AND THEIR IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS (2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf; DIDIER BIGO ET AL., EUR. PARLIAMENT POL'Y DEPT., CITIZENS' RTS. & CONST. AFF., FIGHTING CYBER CRIME AND PROTECTING PRIVACY IN THE CLOUD (2012), *available at* http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050; Judith Rauhofer & Caspar Bowden, *Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud* (Univ. of Edinburgh Sch. of Law, Working Paper No. 2013/28, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2283175; Zack Whittacker, *Patriot Act Can "Obtain" Data in Europe, Researchers Say*, CBS NEWS (Dec. 4, 2012, 5:19 PM), http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say. The EU data protection framework as it relates to trans-border data flows to the United States also plays an important role in this discussion. *See* Memorandum 13/1059 from the Eur. Comm'n on Restoring Trust in EU-US Data Flows (Nov. 27, 2013) (*available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm).

8. *See* Rubinstein et al., *supra* note 2, at 43. For some comparative data, see also WINSTON MAXWELL & CHRISTOPHER WOLF, HOGAN LOVELLS, A GLOBAL REALITY: GOVERNMENTAL ACCESS TO DATA IN THE CLOUD (2012), *available at* http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf.

9. *See, e.g.*, EUR. NETWORK & INFO. SEC. AGENCY, CLOUD COMPUTING 45-46 (Daniele Catteddu & Giles Hogben eds., 2009), *available at* http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

framework.[10] Third, fundamental questions remain and are the subject of official review, such as through the President's Review Group,[11] as to the appropriate standards and related safeguards for lawful access to data of foreign organizations and individuals.[12] Finally, it seems likely that cross border markets and flows of data will continue to grow and intensify in light of the technology and market dynamics underlying cloud computing services. Thus, the challenges for the cloud industry facing these unresolved issues of transnational cloud surveillance are substantial.

B. A Cloud Industry Under Threat

If anything, the Snowden leaks clearly illustrate that global cloud service providers are facing a new class of threats from intelligence agencies across the world. The revelations are many and diverse in nature. This Article proposes that, from the perspective of the cloud industry, the threats can be generally distinguished in terms of *front-door* versus *backdoor* access to data and communications handled by cloud providers. Revelations of front-door access in the U.S. context include PRISM and the widely discussed telephone metadata program.[13] The PRISM program is conducted on the basis of Section 702 of the FISA Amendments Act 2008 (FAA), under which the U.S. intelligence community has successfully gained access to data from U.S. cloud services related to non-U.S. persons reasonably believed to be outside the U.S.[14] Under this program, the NSA gains access by demanding cloud and communication service providers hand over customer information and content, requiring annual certification, and with targeting and minimization procedures reviewed by the Foreign Intelligence Surveillance Court.[15] What is most striking about these programs is the structural basis and scale on which access takes place. In addition, many have raised doubts about the statutory and constitutional basis of these programs under U.S., international, as well as foreign law.[16] Observers and stakeholders from outside of the United States

---

10. *See, e.g.*, Van Hoboken et al., *supra* note 2, at 25-32; Ian Traynor, *New EU Rules to Curb Transfer of Data to U.S. After Edward Snowden Revelations*, THE GUARDIAN, Oct. 17, 2013, 10:13 EDT, http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden; Jefferson Ribeiro, *Bill Would Allow Brazil to Decree Local Internet Data Storage*, REUTERS (Nov. 5th, 2013, 3:34 PM), http://www.reuters.com/article/2013/11/05/net-us-brazil-internet-idUSBRE9A30SI20131105.

11. *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMM'CN TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 153 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter REVIEW GROUP REPORT].

12. One such question is the territorial application of the privacy guarantees of certain human rights treaties. *See* Charlie Savage, *U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad*, N.Y. TIMES, Mar. 7, 2014, at A6, *available at* http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html.

13. *See infra* Part II.C.

14. *See id.*

15. *See* NAT'L SEC. AGENCY, NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 2-3 (Apr. 16, 2014), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf [hereinafter NSA FISA REPORT].

16. For a discussion of legal issues related to Section 702 as the basis for programs like PRISM, see Jennifer Granick, *Reforming the Section 702 Dragnet (Part 1)*, JUST SECURITY (Jan. 30, 2014, 5:24 PM) http://justsecurity.org/2014/01/30/reforming-section-702-dragnet-1. *See generally*, Rubinstein et al.,

are especially troubled by the fact that Section 702 would clearly violate the Fourth Amendment if it were designed to intercept the communications of U.S. persons.[17]

Even more worrying from an industry perspective is that intelligence agencies have begun to gain backdoor access to the data handled by cloud providers. Backdoor access dispenses with serving orders on cloud providers or otherwise notifying them or seeking their cooperation.[18] Reports about a variety of U.S. and British programs show how the intelligence community has systematically sought such backdoor access to data outside of the knowledge of cloud providers. For example, a program known as MUSCULAR apparently enables the NSA to intercept the unencrypted data traffic between cloud provider data centers.[19] Similarly, the UPSTREAM program, details of which were revealed in combination with the revelations about PRISM, showed that the NSA was gaining sweeping access to Internet communications through the targeting of the telecommunications infrastructure.[20] Additionally, the BULLRUN program

---

supra note 2; Van Hoboken et al., *supra* note 2. The Supreme Court reviewed a challenge to Section 702 in *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138, 1150 (2013) (holding that respondents lacked standing to challenge Section 702). However, the Privacy and Civil Liberties Oversight Board (PCLOB), which is a board created by Congress to review and analyze executive branch anti-terrorism efforts and ensure that they are balanced with the need to protect privacy and civil liberties, *see generally* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., http://www.pclob.gov (last visited Apr. 21, 2014), recently issued a report in which it concluded that the metadata program was illegal under U.S. law. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. The PCLOB is currently conducting a similar study of Section 702. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., PUBLIC HEARING REGARDING THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

17. *See* REVIEW GROUP REPORT, *supra* note 11, at 153 ("If Section 702 were designed to intercept the communications of United States persons, it would clearly violate the Fourth Amendment."). *See also* REPORT ON THE FINDINGS BY THE EU CO-CHAIRS OF THE AD HOC EU-US WORKING GROUP ON DATA PROTECTION (2013), *available at* http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf ("US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the U.S."); COMM. ON CIVIL LIBERTIES, JUSTICE & HOME AFFAIRS, EUR. PARLIAMENT, DRAFT REPORT ON THE U.S. NSA SURVEILLANCE PROGRAMME, SURVEILLANCE BODIES IN VARIOUS MEMBER STATES AND THEIR IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS AND ON TRANSATLANTIC COOPERATION IN JUSTICE AND HOME AFFAIRS, 2013/2188(INI) (Jan. 8, 2014), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/moraes_1014703_/moraes_1014703_en.pdf [hereinafter LIBE COMMITTEE DRAFT REPORT]; David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013, 12:48 PM), http://justsecurity.org/2013/10/29/foreigners-nsa-spying-rights; Office of the Press Sec'y, The White House, Presidential Policy Directive on Signals Intelligence Activities (PPD-28) (Jan. 17, 2014) (*available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf) (recognizing "the legitimate privacy and civil liberties concerns of . . .citizens of other nations," while not extending the same protections to them as available for U.S. persons).

18. For the purposes of our discussion, *backdoor* access also covers processes that may be better characterized as involving *side-door* access to data. *See also infra* note 20 and accompanying text.

19. *See infra* notes 117-120 and accompanying text. *See also infra* Part III.B.2.

20. *See infra* notes 112-113 and Part III.B.1 for further discussion of UPSTREAM. This Article categorizes access to cloud data through the telecommunications infrastructure as backdoor access

showed how the NSA had systematically undermined encryption and security in available commercial systems through a variety of covert methods.[21] These methods include the undermining of encryption standards, the covert influence of software design, and the pressuring of industry and firms to hand over encryption keys, thereby allowing for circumvention of security measures more generally.[22] Leaked documents suggest that these programs are conducted pursuant to Section 702 of the FAA as well as Executive Order 12333.[23] The latter sets guidelines for intelligence activities including foreign intelligence gathering conducted abroad, but does not involve any judicial or congressional oversight.[24]

C. The Cloud Industry Responds While Being Caught in the Middle

As discussed in more detail later in this Article, the revelations involving backdoor access have led to the strongest industry response. Most fundamentally, backdoor access programs have forced cloud providers to rethink their relationship with (their own and foreign) governments and to take steps designed to prevent intelligence agencies from gaining unauthorized access to their systems.[25] In other words, when cloud providers implement security measures against unauthorized access, they are forced to consider intelligence agencies as just another third-party adversary whose access they must block.[26] The main difference is one of resources and skills: as compared with any other adversary, intelligence agencies have world-class technology and expertise and seemingly unlimited budgets. Furthermore, cooperation among allied agencies with similar capabilities acts as a force multiplier, as is the case with the "Five Eyes," consisting of the U.S., the U.K., Canada, Australia, and New Zealand.[27]

The international political response to the revelations of large scale

---

because the interception takes place through the targeting of a third party other than the cloud provider, notwithstanding the fact that the intelligence community follows legal processes with respect to the telecommunications providers.

21. For information on the BULLRUN program, *see infra* note 114-116 and accompanying text.

22. *See* Nicole Perlroth, Jeff Larson, & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1, *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html (discussing documents which detail that the N.S.A. spends more than $250 million a year on its Sigint Enabling Project, which "actively engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" to make them "exploitable"). *See also infra* notes 113-116 and accompanying text.

23. Exec. Order No. 12333, 3 C.F.R. 200 (1981).

24. *See infra* notes 152-153.

25. *See infra* Part III.B.2 for a detailed discussion.

26. *See* Smith, *supra* note 2.

27. The Five Eyes collaboration is based on the UKUSA agreements. *See UKUSA Agreement Release 1940-1956*, NAT'L SEC. AGENCY (June 24, 2010), http://www.nsa.gov/public_info/declass/ukusa.shtml. *See generally* JEFFERY T. RICHELSON, THE US INTELLIGENCE COMMUNITY 347-372 (6th ed. 2012). Many of the programs revealed by Snowden involved cooperation between the NSA and the British intelligence agency, Government Communications Headquarters (GCHQ). *See* Nick Hopkins & Julian Borger, *Exclusive: NSA Pays £100m in Secret Funding for GCHQ*, THE GUARDIAN, August 1, 2013, 11:04 EDT, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

transnational surveillance has been significant.[28] Foreign governments, such as Germany and Brazil, have not only sought clarifications from the U.S. but have also started to propose regulatory measures designed to counter it.[29] In the EU-U.S. context, the revelations have complicated ongoing trade negotiations,[30] imperiled the Safe Harbor Program,[31] and emboldened the European Parliament to adopt poison pill amendments to the proposed EU data protection regulation.[32] In the broader international context, Brazil has been particularly vocal about its objections to U.S. spying and, with Germany, sponsored a new United Nations resolution requiring a report on the protection and promotion of privacy "in the context of domestic and extraterritorial surveillance . . . including on a mass scale."[33] Moreover, the U.S. now faces significantly more opposition to its historically dominant position in Internet governance.[34]

In addition, market conditions for U.S. cloud providers have deteriorated as a

---

28. For an overview of responses, see DAVID WRIGHT & REINHARD KREISSL, EUROPEAN RESPONSES TO THE SNOWDEN REVELATIONS: A DISCUSSION PAPER, (2013), *available at* http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.

29. *See, e.g.*, Alison Smale, *Merkel Backs Plan to Keep European Data in Europe*, N.Y. TIMES, Feb. 17, 2014, at A6, *available at* http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html; H. E. Dilma Rousseff, President of the Federative Republic of Brazil, Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly (Sept. 24, 2013) (transcript available at http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf).

30. *See, e.g.*, Joshua Chaffin, *Snooping Claims Add New Complication to Tough EU-US Trade Talks*, FIN. TIMES (June 30, 2013, 6:54 PM), http://www.ft.com/cms/s/0/82026644-e1a1-11e2-b796-00144feabdc0.html#axzz2ytFYLEMd; Press Release, Eur. Parliament, NSA Snooping: MEPs Table Proposals to Protect EU Citizens' Privacy (Feb. 12, 2014) (*available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20140210IPR35501%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN) ("The European Parliament should withhold its consent to an EU-US trade deal unless it fully respects EU citizens' data privacy.").

31. *See* WRIGHT & KREISSL, *supra* note 28, at 18-19.

32. *See* Traynor, *supra* note 10. In particular, Compromise Amendment Article 43a of the European Parliament establishes a regime of oversight of European Data Protection Authorities over government access requests abroad. *See* Compromise Amendments on Articles 30-91, Proposal For a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection), COM(2012)0011–C7 0025/2012–2012/0011(COD) (Oct. 17, 2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

33. *See* Peter James Spielmann, *UN Advances Internet Privacy Rights*, ASSOCIATED PRESS (Nov. 26, 2013, 4:22 PM), http://bigstory.ap.org/article/un-advances-Internet-privacy-rights.

34. *See, e.g.*, MILTON MUELLER & BEN WAGNER, FINDING A FORMULA FOR BRAZIL: REPRESENTATION AND LEGITIMACY IN INTERNET GOVERNANCE (Jan. 15, 2014), *available at* http://www.Internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final.pdf; Milton Mueller, *Do the NSA Revelations Have Anything to Do With Internet Governance?*, THE INTERNET GOVERNANCE PROJECT (Feb. 19, 2014), http://www.Internetgovernance.org/2014/02/19/do-the-nsa-revelations-have-anything-to-do-with-Internet-governance. *See also* Press Release, Internet Corp. for Assigned Names & Numbers, Montevideo Statement on the Future of Internet Cooperation (Oct. 7, 2013) (*available at* https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm).

result of new doubts about the security and privacy of cloud data. The revelations have also dealt a significant blow to the reputation of major Internet industry players, which have seen their brands implicated in the reporting about NSA spying programs.[35] Cloud customers expect providers to reassure them that their data is safe and that firms are taking active steps to respond to these new threats. The U.S. cloud industry not only feels besieged by government agencies seeking access to their systems left and right, but rightly worries that its overseas revenues will dry up due to customer mistrust or new restrictions on market entry.[36] Although the increased emphasis on localization rules and requirements in foreign jurisdictions may smack of protectionism and local government surveillance demands,[37] it further complicates the geopolitical situation facing the U.S. industry.

And yet, despite the difficulty and complexity of these issues, doing nothing is simply not an option for cloud providers operating in international markets. Thus, leading cloud firms have been thrust into legal and policy debates concerning transnational surveillance, both in the U.S. and abroad.[38] In the policy context, industry has pushed with some success for more transparency about cloud surveillance, arguing that "transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers."[39] In particular, industry players have joined calls for new international

---

35. *See, e.g.*, Richard Waters, *Cisco Cites Emerging Markets Backlash on NSA Leaks for Sales Slump*, FT.COM (Nov. 13, 2013), http://www.ft.com/intl/cms/s/0/445c67ce-4cb1-11e3-958f-00144feabdc0.html#axzz2ytFYLEMd; *Cyber Risk Report: September 9-15 2013*, CISCO (Sept. 16, 2013, 7:36 PM), http://tools.cisco.com/security/center/viewCrr.x?alertId=30820.

36. *See, e.g.*, DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 3 (Aug. 2013), *available at* http://www2.itif.org/2013-cloud-computing-costs.pdf (estimating losses of $35 billion for the U.S. cloud industry by 2016); Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, Mar. 21, 2014, at A1, *available at* http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (discussing a variety of ways in which U.S industry is negatively affected in foreign sales in the cloud market); James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, FORRESTER (Aug. 14, 2013), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (estimating the costs to be as high as $180 billion). For further discussion on this topic, see REVIEW GROUP REPORT, *supra* note 11, at 212. *See also* Antonia Blumberg, *Brazil Chooses Saab Jet Deal For Air Force After NSA Spying Sours Boeing Bid*, HUFFINGTON POST (Dec. 18, 2013, 6:20 PM), http://www.huffingtonpost.com/2013/12/18/brazil-saab-jet-deal_n_4469386.html; Richard Waters, *Cisco Cites Emerging Markets Backlash on NSA Leaks for Sales Slump*, FT.COM (Nov. 13 2013, 10:57 PM), http://www.ft.com/intl/cms/s/0/445c67ce-4cb1-11e3-958f-00144feabdc0.html#axzz2ytFYLEMdhttp://www.ft.com/intl/cms/s/0/445c67ce-4cb1-11e3-958f-00144feabdc0.html; Anton Troianovski et al., *NSA Fallout Thwarts AT&T*, WALL ST. J., (Oct. 30, 2013), at B1, *available at* http://online.wsj.com/public/resources/documents/print/WSJ_-B001-20131101.pdf.

37. *See, e.g.*, Michael Scaturro, *The Quest to Build an NSA-Proof Cloud*, THE ATLANTIC (Nov. 21, 2013, 7:00 AM), http://www.theatlantic.com/international/archive/2013/11/the-quest-to-build-an-nsa-proof-cloud/281704 (discussing plans of European leaders to push for a European cloud in the face of Snowden revelations and U.S. dominance in the cloud industry).

38. *See* REFORM GOVERNMENT SURVEILLANCE, http://www.reformgovernmentsurveillance.com (last visited Apr. 21, 2014). *See also* Spencer Ackerman, *Tech Giants Reach White House Deal on NSA Surveillance of Customer Data*, THE GUARDIAN, Jan. 27, 2014, 18:34 EST, http://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data.

39. *See* REFORM GOVERNMENT SURVEILLANCE, *supra* note 38.

agreements and argued for legal reforms domestically.[40] As previously mentioned, and discussed in more depth in Part III, at the technical and organizational level, industry players are responding with the deployment of encryption measures to safeguard their customers' data and there is an increased emphasis on the use of privacy enhancing technologies and innovative architectures for securing their services.

Apparently, the methods of the intelligence community and new requirements that the industry faces abroad may force industry players to adopt new measures that could impact the balance of power between intelligence agencies and their targets. While in the past, firms may have considered certain security and encryption measures too costly or inconvenient to implement, under the post-Snowden calculus, they are now adopting them as a matter of business necessity. This is a sea change and also raises the question of whether and to what extent the intelligence community in the U.S. has the legal means and authority to counteract the pervasive use of measures aimed at restricting lawful access to data.

As noted, this Article contributes to the policy debates regarding transnational surveillance by looking at the possible technical and organizational responses of service providers to such surveillance and their interaction with the relevant legal frameworks. A policy solution to the problems of transnational surveillance is still absent and may require a significant overhaul of an international agreement on the legal frameworks for lawful access of data relating to individuals and organizations in the U.S. and abroad.[41] In the meantime, affected industry players have started to explore solutions in the organizational and technical design of their services.

In addition, the Article explores a related and timely issue, namely, whether existing legal authorities enable the intelligence community to prevent, limit, or modify these industry responses consistent with its intelligence gathering mission. This Article suggests that, even though the current framework allows for some governmental counter measures based on technical assistance provisions and other means, the answer to this question is generally negative. It follows that, if the intelligence community wishes to block or reverse heightened and properly implemented security solutions, it will need to obtain new legal authority from the U.S. Congress. A look into past precedents—such as the mid-90s debate over encryption export controls—suggests that industry may well prevail in this next round in the crypto wars.

This Article proceeds as follows: Part II provides historical background concerning the availability and implementation of strong security measures in the commercial and international context and its impact on lawful access as well as the way in which the legal framework for lawful access for Internet services has developed accordingly. Part III looks at industry reactions to the Snowden revelations by exploring several technical responses in more detail, discussing the

---

40. *Id.*

41. The likelihood of no-spying agreements between for instance the U.S. and Germany is reportedly low. *See* Patrick Donahue & Arne Delfs, *Merkel's No-Spy Ambitions With U.S. May Collapse, Envoy Says*, BLOOMBERG NEWS (Feb. 13, 2014, 9:14 AM), http://www.bloomberg.com/news/2014-02-13/merkel-s-no-spy-ambitions-with-u-s-may-collapse-envoy-says.html (quoting one official in the ongoing negotiations as stating that "[t]he Americans have no interest in giving up their sovereignty in this area").

motivation of these responses as well as their aim and effectiveness. Part IV considers to what extent the U.S. intelligence community—under existing legal authorities—can prevent, undermine, or mitigate these technical responses. This entails an examination of several bodies of law, including the technical assistance provisions in both the comprehensive statute regulating the gathering of foreign intelligence,[42] the omnibus law setting standards for law enforcement access to electronic communications and associated data,[43] and the law requiring telecom carriers to design wiretap-ready equipment.[44] The Article serves as a discussion of what lessons may be learned from earlier confrontations in which industry sought for and won relaxation of encryption export controls despite law enforcement and national security objections. The Article concludes with a number of observations about the future of transnational surveillance and the way in which technology and government responses and counter measures may shape governmental access to the cloud.

II. HISTORICAL BACKGROUND

A. Internet Security

The early days of Internet security may be summed up in one word: neglect. From 1969, when the U.S. government established the ARPAnet with four geographically distributed computers communicating with each other using packet switching techniques,[45] until the early 1980s, when the ARPAnet migrated to TCP/IP as its basic communication protocol,[46] this "network of networks" lacked any formal security mechanisms and relied instead on social norms and reputational sanctions to ensure good behavior.[47] TCP/IP lacked a security layer thereby leaving Internet traffic vulnerable to a range of attacks including spoofing, intrusion, and denial of service.[48] It was not until 1992 that the Internet

42. *See* Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of Titles 8, 18, & 50 of the United States Code).

43. *See* Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522 (2012))

44. *See* Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001-1010).

45. *See generally* JANET ABBATE, INVENTING THE INTERNET (2000).

46. TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It was co-invented by Robert E. Kahn and Vinton Cerf. *See generally* JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING: A TOP-DOWN APPROACH (5th ed. 2009).

47. SIMSON GARFINKEL & GENE SPAFFORD, PRACTICAL UNIX AND INTERNET SECURITY 451-52 (2d ed. 1996) ("In the early days of the ARPANET, . . . [s]ecurity problems were rare: if somebody on the network was disruptive, tracking him down and having him disciplined was a simple matter. In extreme cases, people could lose their network privileges, or even their job . . . . In many ways, the Internet was a large private club. These days the internet is not so exclusive. The Internet has grown so large that you can almost never determine the identity of somebody who is breaking into your system . . . .").

48. *See, e.g.*, Bob Metcalfe, Arpa Network Working Grp., RFC 602: The Stockings Were Hung by the Chimney with Care (1973) *reprinted in* SIMSON GARFINKEL & GENE SPAFFORD, WEB SECURITY AND COMMERCE 79 (2d ed. 2002) (identifying three security problems in the early days of the Internet: lack of security against remote access; unauthorized people using the net; and hackers breaking into

Engineering Task Force (IETF) began to seriously consider what needed to be done to secure the Internet.[49]

By the mid-90s, the ARPAnet had split into a separate (and more secure) military network and a network of scientific and academic computers funded by the National Science Foundation (NSF), called NSFnet.[50] In 1995, NSF completed a phased withdrawal to turn over this non-military network to a consortium of commercial providers, creating the predecessor to the Internet.[51] In the early 90s, Tim Berners-Lee and his colleagues at CERN were inventing the World Wide Web.[52] A short time later, Netscape released the first commercial web browser with a graphical use interface,[53] and the general public began using the Internet and browsing the Web in ever increasing numbers.[54]

As the Internet changed and Internet service providers (ISPs) began offering net access as a service to the public, the level of concern regarding Internet security (and privacy) changed with it. As Vinton Cerf later observed, security and privacy concerns emerged when "the community of users grew from a fairly homogeneous cohort linked by common research interests to a highly heterogeneous, globally distributed population."[55] For example, when ISPs began charging members of the public who wanted to "go online," they had an obvious reason to worry about authentication, because they needed to verify which customers were paying for their services. Moreover, ISPs could not rely on the informal norms of "netiquette" to police their networks; they were offering a commercial service to the public and, therefore, had to take steps to protect their service against the growing menace of network attacks, malware, spam, and password theft.

More generally, the promise of the Internet for transforming the world of commerce, communication, and other domains of societal activity would require an increased focus on security. Thus, pioneering Internet firms like Netscape had a

---

machines and crashing them). *See also* Steven Bellovin, *Security Problems in the TCP/IP Protocol Suite*, 19 COMPUTER COMM. REV. 32 (1989) (analyzing the technical basis for these problems).

49. For an early discussion of Internet Protocol Security (i.e., the protocol suite for securing and encrypting Internet communications), see RANDALL ATKINSON, SIPP ENCAPSULATING SECURITY PAYLOAD (1993); *see also* Randall Atkinson, Naval Research Lab., RFC 1825: Security Architecture for the Internet Protocol (Aug. 1995) (*available at* http://tools.ietf.org/pdf/rfc1825.pdf).

50. *See* ABBATE, *supra* note 45, at 185.

51. *See id.* at 194-99.

52. Berns-Lee and his colleagues developed the initial versions of HTML (Hypertext Markup Language), HTTP (Hypertext Transfer Protocol), and a Web server and browser. *See* KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 257 (1998).

53. *Id.* (discussing the first graphical Web browser known as Mosaic).

54. *See, e.g.*, K.G. COFFMAN & A.M. ODLYZKO, AT&T LABS—RESEARCH, THE SIZE AND GROWTH RATE OF THE INTERNET (1998), *available at* http://www.dtc.umn.edu/~odlyzko/doc/internet.size.pdf.

55. Vinton Cerf, *Foreword* to PETER H. SALUS, CASTING THE NET: FROM ARPANET TO INTERNET AND BEYOND, at ix (1995). Like Vinton Cerf, Robert Kahn acknowledges the early neglect of security but for a different reason:

> It was only many years later when the net became really a public utility of sorts that [dangers, such as viruses, fraud or identity theft] started to show up. We were not really thinking about the dangers of that and perhaps we should have done. I wish we had spent more time on that, but again, in the context of what we were doing, we might not have actually got the project off the ground.

Robert Kahn, *Getting the Net Off the Ground*, BBC NEWS, http://news.bbc.co.uk/1/hi/programmes/click_online/4317521.stm (last updated Mar. 4, 2005, 5:23 PM).

strong business incentive to develop new security protocols that would make the Internet safe for commercial transactions.[56] In 1995, Netscape released an early version of the Secure Socket Layer (SSL) protocol, which underlies secure browsing and soon became "the most widely deployed cryptographic system in the world."[57] SSL and its successor, the Transport Layer Security (TLS) standard, are designed to provide communication security over the Internet using a technique known as public-key cryptography to exchange a symmetric encryption key, which encrypts the data flowing between a browser and a web server.[58] TLS/SSL prevents both eavesdropping and tampering, thereby making it possible for the general public to go online safely for e-commerce, online banking, and other uses of the Internet that warrant security, privacy, and confidentiality.[59] By building TLS/SSL support into its browsers, Netscape (and later all other browser vendors) ensured that the general public could automatically benefit from the significant new developments in cryptography.

As the next Section suggests, however, industry's somewhat belated efforts to secure the Internet clashed with the equally powerful needs of government agencies. For example, both the Federal Bureau of Investigation (FBI) and the NSA were determined to ensure ongoing access to information and communications over the Internet. The FBI routinely seeks access to information and communications to conduct investigations and gather evidence for criminal prosecutions.[60] The NSA, on the other hand, has both an information assurance mission, "preventing foreign adversaries from gaining access to sensitive or classified national security information," and a signals intelligence ("sigint") mission for which it "collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations."[61]

In the mid-90's, industry and government clashed in particular over export controls on encryption. The industry argued that the development and sale of popular U.S. software products with strong encryption capabilities should move forward without regulatory constraints, both to protect the nations' vulnerable information infrastructure and to ensure the success of a vital industry that

---

56. *See* Denise Caruso, *Netscape's Decision to Give Away Code Could Alter the Software Industry*, N.Y. TIMES, Feb. 2, 1998, http://www.nytimes.com/1998/02/02/business/technology-digital-commerce-netscape-s-decision-give-away-code-could-alter.html (describing Netscape's decision to give away its browser for free while charging for its server software).

57. WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 52 (2007).

58. The TLS/SSL protocol enables the communicating parties over the Internet to reliably and securely agree on an encryption standard, before actually communicating their respective messages. For the SSL standards, see *The Secure Sockets Layer (SSL) Protocol Version 3.0*, INTERNET ENG'G TASK FORCE (Aug. 2011), http://tools.ietf.org/html/rfc6101. For the TLS protocol, see *The Transport Layer Security (TLS) Protocol Version 1.2*, IETF TOOLS (Aug. 2008), http://tools.ietf.org/html/rfc5246.

59. IETF TOOLS, *supra* note 58.

60. *See generally* NAT'L RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 81-94 (Kenneth W. Dam & Herbert S. Lin eds., 1996) [hereinafter CRISIS REPORT].

61. *Mission*, NAT'L SEC. AGENCY, http://www.nsa.gov/about/mission/index.shtml (last updated Apr. 15, 2011); *see also* CRISIS REPORT, *supra* note 60, at 94-102.

depended on foreign sales for more than half of its revenues.[62] Law enforcement and intelligence officials insisted that some level of export (and possibly even domestic) controls on encryption were necessary to protect their legitimate interests.[63] Thus began the crypto wars.[64]

B. The Crypto Wars

Cryptography encompasses the use of codes and ciphers to protect valuable or sensitive information from disclosure to unauthorized third parties.[65] Until the 1970s, cryptography was the preserve of the military, foreign diplomats, and spies.[66] Over the next several decades, and thanks to the invention of public-key cryptography by academic researchers working outside the military sphere, cryptography gradually moved into the mainstream of computer technology and electronic commerce.[67] As the Internet became a mainstream communications, media, commercial, political and social tool for individuals, businesses, and governments, software companies and service providers turned to encryption for a variety of security needs. Encryption-based security solutions helped to protect electronic funds transfers, guard proprietary and other sensitive information (including digital content such as books, film, and music), and ensure the privacy and security of personal and business records and communications.[68]

By the early 90's, U.S. software vendors, responding to customer demand for greater security, added encryption functionality to then popular messaging and network programs.[69] At the same time, independent developers like Phil Zimmermann developed Pretty Good Privacy (PGP), a program for protecting the privacy of email using the latest developments in public-key cryptography.[70] By the middle of the decade, Netscape and Microsoft had both added support for SSL to their popular Internet browser and server products, which they wished to distribute both in the U.S. and abroad.[71] Under the State Department's interpretations of the International Traffic in Arms Regulations (ITAR), the export of strong cryptographic products was illegal unless the exporter succeeded in the cumbersome process of obtaining a munitions license.[72] In contrast, the Export Administration Regulations (EAR), administered by the Commerce Department, granted general licenses for exports of mass-market software provided that the

---

62. *See* Ira S. Rubinstein & Michael D. Hintze, *Export Controls on Encryption Software*, *in* COPING WITH U.S. EXPORT CONTROLS 2000, 812 PLI/Comm 505 (Evan R. Berlack & Cecil Hunt eds., 2000), *available at* http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm.

63. *Id.*

64. *See generally* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT-SAVING PRIVACY IN THE DIGITAL AGE (2001).

65. DIFFIE & LANDAU, *supra* note 57, at 11-14.

66. CRISIS REPORT, *supra* note 60, at 53.

67. *See, e.g.*, *id.* at 364-95, 414-20.

68. DIFFIE & LANDAU, *supra* note 57, at 47-52.

69. Rubinstein & Hintze, *supra* note 62.

70. Zimmermann released PGP to the Internet, which made it available overseas in apparent violation of U.S. export controls. *See* LEVY, *supra* note 64, at 287-88.

71. Rubinstein & Hintze, *supra* note 62.

72. *Id.*

software programs had somewhat weaker encryption capabilities.[73]

In light of these regulatory hurdles, the U.S. tech industry began lobbying Congress and the Commerce Department to relax export controls on mass-market software with encryption capabilities, arguing that such controls were both ineffective (due to foreign availability of similar products) and harmful to U.S. industry's competitiveness in worldwide markets.[74] Both the FBI and the NSA countered that the broad dissemination of encryption products would become a major hindrance to their respective missions: strong encryption would prevent them from understanding messages they acquired through surveillance or other means, while even weak encryption, if used on a regular basis, would increase the cost of acquisition and analysis.[75]

Faced with these conflicting viewpoints and arguments, the Clinton Administration sought a middle ground. On April 16, 1993, it announced a NSA-designed, tamper-proof encryption chip (the "Clipper" chip) together with a split-key approach to escrowing keys.[76] More specifically, the Clipper chip used a classified secure algorithm for encryption.[77] Each chip also contained a unique key that was split into two parts at the time of manufacture for deposit with two U.S. government escrow agents, which would provide them to law-enforcement agencies upon presentation of a valid court order.[78] By combining strong security with a key escrow system, the Clinton Administration hoped to balance the competing demands of industry and individuals for highly secure communications, with the needs of law-enforcement agencies.[79] Moreover, the Administration promised that devices incorporating the Clipper chip would be exportable to most countries.[80]

The software Industry rejected the key escrow initiative out of hand, arguing that customer demand for escrowed encryption was lacking and that all such systems were inherently less secure, more costly, and more difficult to use than non-escrowed encryption system.[81] In addition, they argued that the whole idea of a key escrow with U.S.-based or U.S.-approved escrow agents was a non-starter in international markets.[82] Over the next several years, the Administration sought to address industry concerns by experimenting with successive versions of the key-escrow program but to no avail.[83] Rather, a broad coalition of software, hardware, Internet, and telecom companies, trade associations, and public interest groups continued to pursue a multi-pronged effort to liberalize export controls, while

---

73. For a general description of U.S. export controls on encryption software during this period, see *id.*

74. *Id.*

75. CRISIS REPORT, *supra* note 60, at 101.

76. Press Release, The White House, Statement by the Press Secretary (Apr. 16, 1993) (*available at* http://epic.org/crypto/clipper/white_house_statement_4_93.html).

77. *Id.*

78. *Id.*

79. *See id.*

80. Rubinstein & Hintze, *supra* note 62.

81. *Id.*

82. *Id.*

83. *Id.*

opposing mandatory key escrow requirements.[84] During this time, the industry coalition and the Administration turned to Congress for a solution and while House and Senate committees debated and approved several bills, Congress did not enact any encryption legislation.[85] Finally, on September 16, 1999, in the midst of the Gore-Bush presidential campaign, the White House announced a major liberalization of U.S. encryption controls that permitted the export of mass-market software with strong encryption capabilities to non-governmental users in most countries (other than those subject to an embargo) as well as other regulatory changes.[86] Clearly, the government backed down in this round of the crypto wars.[87]

But the Administration had already won an important battle earlier in the crypto wars. In 1992, responding to the growing complexity of the telecom industry and the transition to digital switches, the FBI put forth what it called the Digital Telephony Proposal, which would require telecommunications providers to help facilitate government interceptions of wire and electronic communications.[88] Two years later, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) despite industry objections based on costs, loss of privacy, and loss of industry control over the design of its services.[89] Notably, Silicon Valley firms won an important concession: CALEA requirements would apply only to telecommunication services or facilities that enable a subscriber to make, receive, or direct calls, and not to "information services" such as e-mail providers and ISPs.[90] In recent years, the FBI has sought to expand CALEA to Internet services, arguing that the original legislative carve out created a gap between its legal authority and the capabilities of Internet services to comply with wiretap and related orders in a timely and efficient manner, a problem it refers to as "Going Dark."[91] In 2010, the FBI first floated a proposal, dubbed CALEA II, that would extend the technical design mandates of CALEA to a broad range of Internet communications services.[92] Given the controversial nature of the Snowden

---

84. *Id.*

85. *Id.*

86. *Id.*

87. *See generally* A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15 (1996); DIFFIE & LANDAU, *supra* note 57; LEVY, *supra* note 64.

88. DIFFIE & LANDAU, *supra* note 57, at 205-206.

89. *Id.*

90. *See infra* Part IV.A.

91. *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies, Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 10 (2011) (prepared statement of Valerie Caproni, Gen. Counsel, Fed. Bureau of Investigation).

92. *See* Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html ("[O]fficials want Congress to require all services that enable communications—including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype—to be technically capable of complying if served with a wiretap order."). As recently as last spring, the FBI renewed its proposal for a so-called "CALEA II." *See* Charlie Savage, *U.S. Weighing Wide Overhaul of Surveillance*, N.Y. TIMES, May 8, 2013, at A1, *available at* http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html. For a critique of CALEA II, see Joseph Lorenzo Hall, *Leading Security Experts Say FBI Wiretapping*

revelations regarding NSA surveillance methods (discussed below), it seems unlikely that the Obama Administration will have the necessary political support to enact any bill encompassing the FBI's CALEA II proposal.

C. Post-9/11: From Surveillance Reforms to the Snowden Revelations

The two preceding Sections demonstrate how security, encryption, and surveillance intersected in the early history of the Internet and during the crypto wars. They intersected again, and even more dramatically, in the period beginning immediately after the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon and ending with the Snowden revelations and their aftermath. Seven weeks after the 9/11 attacks, Congress passed a new law greatly expanding the government's electronic surveillance powers under FISA, ECPA, and other surveillance laws: the USA PATRIOT Act.[93] Among other things, this act added a broad new definition of terrorism, authorized delayed notice of search warrants, expanded the definition of pen registers, authorized "roving" wiretaps, and permitted FISA applications even where foreign intelligence gathering was not the primary purpose of the investigation (as long as it was a "significant purpose").[94] In addition, Section 215 of the USA PATRIOT Act added a new provision to FISA authorizing the bulk collection and querying of telephone records.[95]

In 2005, *The New York Times* reported that President Bush had issued executive orders, as part of a surveillance program entitled the Terrorist Surveillance Program (TSP), authorizing the NSA to conduct warrantless surveillance of telephone calls and emails from the U.S. to recipients abroad.[96] Not surprisingly, multiple lawsuits and Congressional hearings ensued, challenging the legal validity of TSP and seeking reforms of FISA.[97] In order to immunize the telephone companies that had cooperated with the NSA against liability and provide a legal foundation for intercepting communications where one party was located outside the U.S. and another party inside the U.S., Congress revisited FISA in 2007 and again in 2008.[98] The second revision significantly broadened the

---

Proposal Would Undermine Cybersecurity, CTR. FOR DEMOCRACY & TECH. (May 17, 2013), https://www.cdt.org/blogs/joseph-lorenzo-hall/1705leading-security-experts-say-fbi-wiretapping-proposal-would-undermine-cybersecurity.

93. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified mainly in scattered sections of Titles 8, 18, 28, 42, 49 & 50 of the United States Code). *See also* the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (codified at 50 U.S.C. § 1801(b)(1) (2012)) (creating FISA surveillance authority to target unaffiliated foreign persons who may pose terrorist threats).

94. For an overview of the USA PATRIOT Act, see Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

95. *See* 50 U.S.C. § 1881 (2012).

96. James Risen & Eric Lichtblau, *Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say*, N.Y. TIMES, Dec. 15, 2005, http://www.nytimes.com/2005/12/15/politics/15cnd-program.html?pagewanted=all.

97. *See generally* G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861 (2014).

98. *Id.* at 934-35.

government's power to engage in foreign surveillance.[99] In particular, Section 702 of the FAA authorized senior government officials to target the electronic communications of persons "reasonably believed to be located outside the United States" [100] without having to establish probable cause or seek the approval of the Foreign Intelligence Surveillance Court (FISC)[101] of its decisions about which individuals to target, even if the interception takes place inside the United States.[102] Rather, Section 702 authorizes the FISC to approve annual certifications submitted by senior officials that identify certain categories of foreign intelligence targets whose communications may be collected, subject to FISC-approved targeting and minimization procedures.[103]

On June 5, 2013, the British newspaper *The Guardian* broke the first of many stories involving the "Snowden revelations."[104] The leaks revealed—and continue to reveal—that multiple U.S. government collection and surveillance programs are seemingly beyond the scope of Sections 215 of the USA PATRIOT Act and 702 of the FAA. The first article described an NSA program to collect millions of calling records of U.S. customers of Verizon, regardless of whether they are suspected of any wrongdoing. This program involved the government collection of "telephony metadata" (but not the content of phone calls) on an ongoing basis, subject to the terms of a court order pursuant to Section 215.[105] The next day, *The Guardian* reported on another NSA program referred to in the leaked documents as "PRISM," under which the government collects the content of electronic communications, including "search history, the content of emails, file transfers and live chats."[106] One of the leaked documents suggested that the government was collecting this data directly from the servers of leading U.S. companies including Google, Facebook, and Apple, although the government and the companies involved have all denied such claims.[107]

---

99. *See* FISA Amendments Act of 2008 (FAA), Pub. L. No. 110-261, 122 Stat. 2436 (codified in scattered sections of Title 50 of the United States Code).

100. 50 U.S.C. § 1881a(a) (2012).

101. *See id.* § 1881a(i).

102. *See id.* § 1881a(d).

103. *See id.* § 1881a(g). The FAA also authorized senior officials to issue directives requiring electronic communications service providers to assist the government in collecting these communications. *Id.* §1881a(h).

104. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2103, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

105. *Id*. "Metadata" includes communications routing information such as originating and terminating telephone number and time and duration of call but does not include the contents of communications. Press Release, Director of National Intelligence Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information.

106. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

107. *See* Mark Zuckerberg, *Status Update, June 7, 2013, 5:45 PM*, FACEBOOK (last visited May 7, 2014), https://www.facebook.com/zuck/posts/10100828955847631; Larry Page & David Drummond, *What the ...?*, OFFICIAL GOOGLE BLOG (June 7, 2013), http://googleblog.blogspot.co.uk/2013/06/what.html. *See also* Declan McCullagh, *No Evidence of NSA's 'Direct Access' to Tech Companies*,

These and other Snowden revelations ignited a firestorm of criticism. The leaks sparked what many consider a long overdue debate on the nature and extent of the NSA's surveillance programs and their impact on civil liberties, both in the U.S. and abroad.[108] In the view of many, the revelations also caused immediate damage to U.S. foreign relations[109] and national security.[110] Additionally, the U.S. tech industry—and especially companies in the cloud computing industry—worried about potential spillover damage based on foreign businesses and governments threatening not to use their services because of concerns over NSA spying.[111] And they had good reason for these concerns. Over the course of the next several months, there were at least three additional press reports that undermined U.S. cloud services in the eyes of foreign customers. First, in August 2013, *The New York Times* described another program conducted under Section 702 in which the NSA acquires communications by "systematically searching—without warrants—through the contents of Americans' communications that cross the border . . . temporarily copying and then sifting through the contents of what is apparently most [international] e-mails and other text-based communications."[112] This is sometimes referred to as *upstream* collection, because it apparently involves real-time interception of communications as they pass through fiber cables or other major data pipelines.[113]

A month later, *The New York Times* reported that the NSA has been engaged in and winning a "secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age."[114] This program, which the leaked documents refer to as BULLRUN,[115] is especially significant for present purposes because it reveals how NSA overcame its defeat in

---

CNET (June 7, 2013), http://news.cnet.com/8301-13578_3-57588337-38/no-evidence-of-nsas-direct-access-to-tech-companies.

108. *See infra* Part III.A.

109. *See, e.g.*, Peter Grier, *Are Edward Snowden NSA Leaks Messing up U.S. Foreign Relations?* CHRISTIAN SCI. MONITOR, Sept. 3, 2013, http://www.csmonitor.com/USA/DC-Decoder/Decoder-Buzz/2013/0903/Are-Edward-Snowden-NSA-leaks-messing-up-US-foreign-relations.

110. *See, e.g.*, Ken Dilanian & Richard A. Serrano, *Snowden Leaks Severely Hurt U.S. Security, Two House Members Say*, L.A. TIMES, Jan. 9, 2014, http://articles.latimes.com/2014/jan/09/nation/la-na-snowden-intel-20140110.

111. See *supra* notes 35-37 and accompanying text.

112. Charlie Savage, *Broader Sifting Of Message Data By N.S.A. Is Seen*, N.Y. TIMES, Aug. 8, 2013, at A1, *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all&_r=2&.

113. Craig Timberg, *The NSA Slide You Haven't Seen*, WASH. POST, July 10, 2013, http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html. A study for the European Parliament picked up on the term and concluded that the practice of "upstreaming" appears to be a relatively widespread feature of surveillance by several EU member states. EUR. PARLIAMENT STUDY, NATIONAL PROGRAMMES FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW 19-20 (Oct. 2013), *available at* http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

114. Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1, *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

115. *Id.*

the key escrow and export control debates by finding new ways to exploit vast amounts of encrypted online data. BULLRUN relied on a number of stealthy methods ranging from the use of superfast computes to break codes, to allegedly pressuring companies into handing over their master encryption keys or building in backdoors, to introducing technical weaknesses covertly into commercial encryption standards.[116]

Finally, in October, the *Washington Post* reported that the NSA "has secretly broken into the main communications links that connect Yahoo and Google data centers around the world."[117] Whereas PRISM apparently provided front-door access to Yahoo and Google accounts through a court-approved process under Section 702 of the FAA, this alternative program, called MUSCULAR, intercepted Yahoo and Google data flows through the backdoor as they transited the companies' private fiber-optic networks.[118] In public statements, the companies expressed their "outrage"[119] and, in the wake of these revelations, analysts predicted that U.S. tech companies may lose as much as $180 billion by 2016 due to international concerns about NSA's spying.[120]

III. INDUSTRY RESPONSES AND TECHNICAL SOLUTIONS

A. The Response to Snowden Revelations

The Snowden revelations have led to a wide variety of responses by different actors affected by government access to data and communications processed by cloud providers. Although this Section focuses primarily on the response of cloud providers, it is useful to first consider the wider context by examining the responses of a few selected groups such as security engineers, and the privacy advocacy and human rights community.

Due to the repercussions for information security products and solutions, members of the security engineering community have been particularly vocal in their condemnation of the methods used to gain access to Internet data by corrupting Internet security standards. This community has also played a major role in interpreting and analyzing the technical aspects of the programs that were revealed by Snowden and their implications for the privacy and security of

---

116. *Id.* In certain respects, however, BULLRUN is nothing new. For earlier discussion of how governments in the post-9/11 era are increasingly dependent on the private sector to assist them in collecting and analyzing data for national security purposes, see Jon D Michaels, *Deputizing Homeland Security*, 88 TEX. L. REV. 1435 (2010); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901 (2008).

117. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Show*, WASH. POST, Oct. 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

118. *Id.*

119. *Id.*

120. Mathew J. Schwartz, *NSA Surveillance Fallout Costs IT Industry Billions*, INFORMATION WEEK (Nov. 27, 2013, 1:10 PM), http://www.informationweek.com/security/security-monitoring/nsa-surveillance-fallout-costs-it-industry-billions/d/d-id/1112838.

communications, providing input for the public debate.[121]

Edward Felten, a professor of computer science and public policy, and former Chief Technologist for the Federal Trade Commission, noted that "[i]n security, the worst case . . . is thinking you are secure when you're not. And that's exactly what the NSA seems to be trying to perpetuate."[122] Bruce Schneier, a leading computer security specialist who has written extensively about the Snowden documents, echoed a broader sentiment in castigating the NSA for its "betrayal" of security engineers and free and open nature of the Internet.[123] Debates are already underway within the IETF and the World Wide Web Consortium (W3C) on how best to counter the threats of pervasive monitoring and are likely to result in new and improved Internet security standards and practices.[124]

Privacy advocacy groups around the world have used the Snowden revelations to intensify ongoing campaigns to limit government surveillance of Internet users. First, these groups have filed a number of court cases in the U.S. and abroad, including in the U.K., Germany, and the Netherlands.[125] Within the international human rights community, there are several new initiatives to strengthen safeguards against government surveillance. For example, the Inter-American Commission on Human Rights held an official hearing on the NSA's mass surveillance programs.[126] Additionally, in July 2013, a broad international coalition of more than four hundred human rights related NGOs finalized and signed the International Principles on the Application of Human Rights to Communications

---

121. *See, e.g.*, Martín Abadi et al., An Open Letter from U.S. Researchers in Cryptography and Information Security (Jan. 24, 2014) (*available at* http://masssurveillance.info/openletter.pdf); Ben Adida et al., Technologists' Comment to the Director of National Intelligence Review Group on Intelligence and Communications Technology (Oct. 4, 2013) (*available at* https://www.cdt.org/files/pdfs/nsa-review-panel-tech-comment.pdf).

122. Ed Felten, *NSA Apparently Undermining Standards, Security, Confidence*, FREEDOM TO TINKER (Sept. 9, 2013), https://freedom-to-tinker.com/blog/felten/nsa-apparently-undermining-standards-security-confidence.

123. Bruce Schneier, *The U.S. Government Has Betrayed the Internet. We Need to Take it Back*, THE GUARDIAN, Sept. 5, 2013, 5:04 EST, http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-Internet-nsa-spying.

124. *See, e.g.*, Jari Arkko & Stephen Farrell, *Security and Pervasive Monitoring*, IETF (Sept. 7, 2013), https://www.ietf.org/blog/2013/09/security-and-pervasive-monitoring. For the W3C, see *A W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT) Internet(Feb. 28—Mar. 1, 2014)*, WORLD WIDE WEB CONSORTIUM, https://www.w3.org/2014/strint/report.html (last visited May 7, 2014).

125. In the United States, there have been several cases filed against the meta-data collection program based on Section 215. *See* Spencer Ackerman & Dan Roberts, *NSA Phone Surveillance Program Likely Unconstitutional, Federal Judge Rules*, THE GUARDIAN, Dec. 16, 2013, 15:38 EST, http://www.theguardian.com/world/2013/dec/16/nsa-phone-surveillance-likely-unconstitutional-judge. For an overview of ongoing litigation about NSA surveillance, see Kara Brandeisky, *NSA Surveillance Lawsuit Tracker*, PROPUBLICA, http://projects.propublica.org/graphics/surveillance-suits (last updated Feb. 24, 2014). For a short overview and references to important cases in the wake of the Snowden revelations in Europe, see Axel Arnbak, *ECHR Fast-tracks Court Case on PRISM and TEMPORA (and VERYANGRYBIRDS?)*, FREEDOM TO TINKER (Jan. 29, 2014), https://freedom-to-tinker.com/blog/axel/echr-fast-tracks-court-case-on-prism-and-tempora-and-very-angry-birds.

126. Steven M. Watt, *International Rights Body to Press U.S. on Surveillance, Snowden*, ACLU BLOG OF RTS. (Oct. 25, 2013), https://www.aclu.org/blog/national-security-human-rights/international-rights-body-press-us-surveillance-snowden.

Surveillance ("Principles").[127] The Principles condemn mass surveillance as a human rights violation and assert and interpret accepted principles such as proportionality, necessity, and transparency in the communications surveillance context.[128] Finally, a broad range of NGOs have joined forces in the Stop Watching Us[129] coalition and the more recent 'Day We Fight Back.'[130] The international human rights community has also condemned the treatment of Edward Snowden as a criminal rather than as a whistleblower and condemned restrictions on the reporting of the leaked documents.[131] In a recent report, Frank La Rue, the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, analyzed the implications of mass surveillance on the right to freedom of expression and the need for government surveillance practices to comply with human rights standards.[132]

B. The Industry Response: Taking Care of Old Business

In a recent article, reporter Steven Levy nicely captures the general response of Internet firms to the Snowden revelations by providing a look "inside their year from hell."[133] Levy documents industry's struggle to craft a proper response to the uproar about direct government access to their servers (as alleged in the early reports of PRISM) and reassure overseas customers in light of the unhelpful U.S. government statements that NSA snooping was only directed at "non-American citizens."[134] Industry had little success in quelling suspicion and regaining trust, especially from foreign customers and governments. "Every time we spoke it seemed to make matters worse . . . [w]e just were not believed," explained one tech executive to Levy.[135]

Quite apart from overcoming this atmosphere of general distrust, industry players had enough on their hands in deciding on a practical response to the Snowden troubles. Of the many possible technical measures aimed at restricting undue access to online information and communication, the most obvious one for them to consider was more extensive use of encryption. When properly implemented by cloud providers, encryption measures can help secure

---

127. *See International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (July 10, 2013), https://en.necessaryandproportionate.org/text.

128. *Id.*

129. *See* STOP WATCHING US, https://optin.stopwatching.us (last visited May 7, 2014).

130. *See* THE DAY WE FIGHT BACK, https://thedaywefightback.org (last visited May 7, 2014).

131. *See, e.g.*, *USA Must Not Persecute Whistleblower Edward Snowden*, AMNESTY INTERNAT'L (July 2, 2013), http://www.amnesty.org/en/news/usa-must-not-persecute-whistleblower-edward-snowden-2013-07-02.

132. Frank La Rue issued a report just one day before the first Snowden leaks in June 2013. *See* U.N. GAOR, 23rd Sess., U.N. Doc. A/HRC/23/40 (Apr. 17, 2014), *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

133. Steven Levy, *How the NSA Almost Killed the Internet*, WIRED (Jan. 7, 2014, 6:30 AM), http://www.wired.com/threatlevel/2014/01/how-the-us-almost-killed-the-internet/all/.

134. *See* Tomio Geron, *Mark Zuckerberg: U.S. Government 'Blew It' On NSA Issue*, FORBES (Sept. 11, 2013, 7:20 PM), http://www.forbes.com/sites/tomiogeron/2013/09/11/live-mark-zuckerberg-speaks-at-techcrunch-disrupt.

135. Levy, s*upra* note 133.

communications and stored data against third party intrusions, including those of government intelligence agencies.[136] At the very least, service providers could deploy encryption protocols like TLS/SSL to secure client-server communications between users and their own services.[137] The MUSCULAR revelations suggest that service providers could also encrypt data more comprehensively once it arrives at their servers for processing or storage.[138] Indeed, many of the measures discussed in this Section are but old wine in new bottles: that is, prudent responses to longstanding security risks that have been given greater urgency by the Snowden revelations. If the cloud industry had taken information security more seriously years ago, their services would have been less vulnerable in the first place.

Before turning to the specifics of the industry responses, it is worth briefly observing that despite the value of encryption measures in hindering surveillance, it has some limitations. In particular, as long as a service provider holds or has access to its users' encryption keys, it maintains the ability to access a user's data in unencrypted form, notwithstanding the fact that data travels between a client and a server securely. Moreover, for encryption measures to be effective in preventing backdoor access, industry must rely on cryptographic standards and implementations that have not been corrupted and must keep encryption keys out of the hands of government agencies. This may seem obvious, but achieving it is less so. Recent revelations related to NSA efforts to undermine cryptographic standards themselves are particularly worrying in this regard.[139]

In its discussion of what should be done to promote security and trust in encryption technologies, the President's Review Group implicitly rejected NSA activities undermining encryption standards by recommending that the U.S. Government should: "(1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."[140] While specific implementations of encryption technologies may suffer from security weaknesses, the use of encryption generally helps protect cloud data against interception by third parties, including government agencies. In contrast, no encryption or weak

---

136. *See supra* Part II.

137. *See id.; see also* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Backdoors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359 (2010).

138. *See supra* notes 117-120 and accompanying text.

139. After revelations about the corruption of the DUAL-EC standard by the NSA, the National Institute of Standards and Technology (NIST) responded by advising against the use of this standard. *See* Office of the Dir., *Cryptographic Standards Statement*, NIST (Sept. 10, 2013), http://www.nist.gov/director/cybersecuritystatement-091013.cfm. More recently, NIST launched a review of its standards development process to address concerns about the security and integrity of NIST cryptographic standards. *See* Computer Sec. Div., *NIST Initiating Review of Cryptographic Standards Development Process*, NIST (Feb. 18, 2014), http://csrc.nist.gov/groups/ST/crypto-review.

140. *See* REVIEW GROUP REPORT, *supra* note 11, at Recommendation 29. The Review Group has been criticized for being vague in its factual review of NSA activities related to cryptographic standards and software backdoors more generally. *See* Ed Felten, *Software Backdoors and the White House NSA Panel Report*, FREEDOM TO TINKER (Dec. 19, 2013), https://freedom-to-tinker.com/blog/felten/software-backdoors-and-the-white-house-nsa-panel-report.

encryption enables government agencies to access cloud data without having to rely on legal process directed at cloud providers or the targeted interception of key material.

1. Securing Communications between Users and Cloud Services

As recently as five years ago, most of the best known and free cloud services failed to encrypt the communications channel they used to transmit data to and from their users. As a result, anyone gaining access to this communication channel could easily intercept private communications between the users and the service. Nor was it difficult to gain access given the combination of readily available interception software and insecure computing environments.[141]

More recently, many of the major web-based cloud providers have begun to implement and enable by default standard encryption protocols, including the Hypertext Transfer Protocol Secure (HTTPS), which has been pervasive in the field of ecommerce and online banking for many years. The Snowden revelations and the apparent massive collection of Internet communications content through programs such as UPSTREAM clearly demonstrate the value of encrypted communications between users and cloud providers. When implemented properly, HTTPS ensures that the communications between the browser and the web-based service are secure from third party access.[142] The protocol achieves this in two ways: first, it authenticates the identity of the service, and, second, it uses SSL/TLS to encrypt the data that subsequently flows between a user and this service.[143] Some services have taken additional steps to protect their users from government surveillance by implementing protocols with "perfect forward secrecy," which is a property of certain encryption protocols that ensures that if an encryption key, which, if is compromised, past messages with the user remain uncompromised.[144]

Cost is the main reason that service providers delayed adopting this industry standard for cloud services. Browsers have long supported the use of secure connections by users, but securing all the connections by default requires that cloud services increase their server-side processing capacity. However, as market dynamics are now beginning to show, the costs for such encryption measures are not prohibitive. The transition of web-based cloud service providers to HTTPS by default is now ongoing. Google, Microsoft and Facebook have already enabled

---

141. Shared Internet access points, such as in Internet cafes, are often insecure and security practices of most users would clearly warrant the enabling of security by default. For a discussion of security issues related to cloud services in 2009, see Ryan Singel, *Encrypt the Cloud, Security Luminaries Tell Google*, WIRED (Jun. 16, 2009), http://www.wired.com/threatlevel/2009/06/google_ssl. The expert letter discussed in the Singel article details a variety of security issues for users of Google's cloud services due to the absence of SSL by default. *See* Letter from Alessandro Acquisti et al., to Eric Schmidt, CEO Google, Re: Ensuring Adequate Security in Google's Cloud Based Services (June 2009) (*available at* http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf).

142. *See* DAVID GOURLEY ET AL., HTTP: A DEFINITIVE GUIDE 202-10, 308 (Linda Mui, ed., 2002).

143. *Id.* at 308.

144. *See* Parker Higgins, *Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection*, ELEC. FRONTIER FOUND. (Aug. 28, 2013), https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection.

HTTPS.[145] One of the last major U.S. based web companies to respond to calls for implementation of HTTPS by default is Yahoo, which announced plans to start implementing it by early 2014.[146]

In terms of securing web-based communications, however, the HTTPS system is no panacea against government surveillance. First, the protocol must be properly implemented.[147] Second, there are known attacks on the use of encrypted web communications through SSL.[148] Third, intelligence agencies may work around the protections and attempt to secretly install software on the computers of targeted users, thereby allowing them to capture their communications before they are transmitted across an encrypted connection.[149] Finally, and most importantly, HTTPS is not designed to protect data at rest. Even if a cloud provider properly implements this protocol, this does nothing to prevent a government agency from obtaining the data it seeks by means of a compulsory order requiring the service provider to furnish this data. Indeed, as Professor Peter Swire argues, the trend towards encrypting data in transit between users and cloud services may well result in governments shifting their attention from attacking the communication infrastructure to demanding that cloud service providers hand over stored data after it has been securely transmitted.[150] The Snowden revelations already provide some

---

145. *See, e.g.*, Sam Schillace, Gmail Engineering Director, *Default HTTPS Access for Gmail*, OFFICIAL GMAIL BLOG (Jan. 12, 2010), http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html; Dick Craddock, Grp. Program Mgr. for Windows Live Hotmail, *Hotmail Security Improves with Full-Session HTTPS Encryption*, THE WINDOWS BLOG (Nov. 9, 2010), http://blogs.windows.com/windows_live/b/windowslive/archive/2010/11/09/hotmail-security-improves-with-full-session-https-encryption.aspx; Dick Craddock, Grp. Program Mgr., Hotmail, *An Update on SSL Support*, THE WINDOWS BLOG (July 7, 2011), http://blogs.windows.com/windows_live/b/windowslive/archive/2011/07/07/an-update-on-ssl-support.aspx; Antone Gonsalves, *Facebook Praised For Encrypting Web Access By Default*, CSO ONLINE (Nov. 20, 2012), http://www.csoonline.com/article/721978/facebook-praised-for-encrypting-web-access-by-default.

146. *See* Liam Tung, *Yahoo Finally Enables HTTPS Encryption for Email by Default*, ZDNET (Jan. 8, 2014), http://www.zdnet.com/yahoo-finally-enables-https-encryption-for-email-by-default-7000024922.

147. There are a wide variety of security issues in the implementation phase of these protocols, a discussion of which is beyond the scope of this Article. For a recent example detailing problems relating to the choices of large prima numbers in public key RSA cryptographic protocols, see Arjen K. Lenstra et al., *Ron was Wrong, Whit is Right*, 2012 IACR CRYPTOLOGY EPRINT ARCHIVE 64 (2012), *available at* http://eprint.iacr.org/2012/064.pdf.

148. *See, e.g.*, Ivan Ristić, *SSL Threat Model*, BLOG: IVAN RISTIĆ (Sept. 9, 2009), http://blog.ivanristic.com/2009/09/ssl-threat-model.html. *See also* Nevana Vratonjic et al., *The Inconvenient Truth about Web Certificates*, WORKSHOP ON THE ECON. OF INFO. SEC. (2011), http://weis2011.econinfosec.org/papers/The%20Inconvenient%20Truth%20about%20Web%20Certificates.pdf.

149. *See, e.g.*, Ryan Gallagher & Glenn Greenwald, *How the NSA Plans to Infect 'Millions' of Computers with Malware*, THE INTERCEPT (Mar. 12, 2014), https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware (detailing an expansion by the NSA of its ability to gain access and control over millions of computers worldwide). The NSA responded with a public statement that the reports were inaccurate. *See* Press Release, Pub. Affairs Office, Nat'l Sec. Agency, Statement in Response to Press Allegations (Mar. 13, 2014) (*available at* http://www.nsa.gov/public_info/_files/speeches_testimonies/2014_03_14_press_allegations_response.pdf).

150. Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 INT'L DATA PRIVACY L. 200 (2012).

evidence of this shift and the measures detailed in this Section could accelerate this trend. To counter this trend, governments confronted with encrypted communication channels could try to compel cloud providers to hand over their encryption keys, enabling the continued effective interception over telecommunications infrastructure (an option discussed further in Part IV).

2. Securing Information Flows Between Data Centers

The MUSCULAR revelations indicate that intelligence agencies are also systematically gaining access to cloud data through the targeting of the communications links between cloud provider data centers.[151] Taken at face value, MUSCULAR suggests that the NSA has engaged in efforts to circumvent online security measures and surreptitiously collect customer data without serving legal process either on cloud providers or directly on customers themselves. This does not necessarily imply that programs like MUSCULAR have no basis in the law. Rather, it seems likely that the NSA conducts this program under the terms of Executive Order 12333,[152] which is the principal governing authority for U.S. intelligence activities outside the United States.[153]

Nevertheless, industry has reacted very negatively to the NSA's use of methods associated with the MUSCULAR program. For example, Google's General Counsel, David Drummond, stated that his company was "outraged at the

---

151. *See supra* Part II.

152. Exec. Order No. 12333, 3 C.F.R. 200 (1981). Exec. Order No. 12333 was amended in part by Exec. Order No. 13284, 68 Fed. Reg. 3371 (Jan. 23, 2003), by Exec. Order No. 13355, 69 Fed. Reg. 53593 (Aug. 27, 2004), and further amended by Exec. Order No. 13470, 73 Fed. Reg. 45325 (July 30, 2008).

153. Exec. Order No. 12333 provides that "[t]imely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States." It declares that "special emphasis should be given to detecting and countering" espionage, terrorism, and the development, possession, proliferation, or use of weapons of mass destruction. The executive order directs that "such techniques as electronic surveillance" may not be used "unless they are in accordance with procedures . . . approved by the Attorney General" and that "[s]uch procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes." Exec. Order No. 12333, 3 C.F.R. 200 (1981). For a brief description of the (limited) privacy protections under Exec. Order No. 12333, see REVIEW GROUP REPORT, *supra* note 11, at App. B (describing limitations on targeting, collection, analysis, dissemination, and retention). It is an interesting question whether such activity is also lawful under international law and it is quite possible that certain types of U.S. foreign intelligence gathering, while permitted under U.S. law, could be unlawful in the foreign territory where they are conducted. For a discussion, see Van Hoboken et al., *supra* note 2; Brown & Korff, *supra* note 6. The Snowden revelations have reignited a debate about the extraterritorial scope of human rights treaties, a feature the U.S. Government has resisted. *See* Beth van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change*, 90 INT'L L. STUD. 20 (2014); Letters to the Editor, *Letter to the Editor from Former Member of the Human Rights Committee, Martin Scheinin*, JUST SECURITY (Mar. 10, 2014), http://justsecurity.org/2014/03/10/letter-editor-martin-scheinin; Marko Milanovic, *Foreign Surveillance and Human Rights, Part 2: Interpreting the ICCPR*, EJIL: TALK! (Nov. 26, 2013), http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-2-interpreting-the-iccpr; Charlie Savage, *U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad*, N.Y. TIMES, Mar. 7, 2014, at A6, *available at* http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html.

lengths to which the government seems to have gone" to gain access to customers' data.[154] At the same time, Drummond viewed MUSCULAR as a "very logical explanation" of the apparent discrepancy between the "massive amount of data" NSA reportedly held and the "small amount of data" that Google and others in the industry have been providing.[155] Drummond's response suggests dissatisfaction with MUSCULAR, at least in part because it removes industry from the government data gathering process. Rather, industry statements suggest that government data access should respect a service provider's organizational and technical infrastructure. Similarly, Microsoft's General Counsel, Brad Smith, contends that, except in rare circumstances, government should access customer data through the front door by serving legal process on the cloud service provider or its customers.[156] Based on the revelation of MUSCULAR and similar programs, Smith stated that government snooping constitutes "an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks."[157]

It is hardly surprising, then, that cloud firms like Microsoft have started taking steps to ensure that governments use legal process rather than "technological brute force to access customer data."[158] Microsoft recently announced "a comprehensive engineering effort to strengthen the encryption of customer data across [its] networks and services."[159] This matches similar activity of Google, which had started to encrypt data more comprehensively even before the specific revelations about the MUSCULAR program.[160] As a Google security engineer explained shortly after these revelations, "the traffic shown in the [MUSCULAR] slides below is now all encrypted and the work the NSA/GCHQ (U.K. Government Communications Headquarters) staff did on understanding it, ruined."[161] Finally, Yahoo has announced it will "[e]ncrypt all information that moves between [its] data centers by the end of Q1 2014."[162] The encryption measures discussed above could help the cloud industry to counteract programs like MUSCULAR and UPSTREAM, which rely on the bulk collection of data by targeting communication links and the telecommunications infrastructure. Of course, this assumes that the NSA does not seek to undermine these protections by relying on security weaknesses in the implementation or use of SSL or the underlying encryption

---

154. *See* Levy, *supra* note 133.

155. *Id.*

156. *See* Smith, *supra* note 2.

157. *Id.*

158. *Id.*

159. *Id.*

160. *See* Craig Timberg, *Google Encrypts Data Amid Backlash Against NSA Spying*, WASH. POST, Sept 6, 2013, http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html.

161. Mike Hearn, *Posting to Google+*, GOOGLE+ (Nov. 5, 2013), https://plus.google.com/+MikeHearn/posts/LW1DXJ2BK8k. *See also* Jennifer Garnett, *Google Encrypts Its Network to Counteract NSA Surveillance*, JOLT DIGEST (Nov. 18, 2013), http://jolt.law.harvard.edu/digest/privacy/google-encrypts-its-network-to-counteract-nsa-surveillance. *See also* Nicolas Lidzborski, Gmail Security Engineering, *Staying at the Forefront of Email Security and Reliability: HTTPS-Only and 99.978 Percent Availability*, GOOGLE BLOG (Mar. 20, 2014), http://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html?m=1.

162. Marissa Mayer, *Our Commitment to Protecting Your Information*, YAHOO (Nov. 18, 2013), http://yahoo.tumblr.com/post/67373852814/our-commitment-to-protecting-your-information.

algorithms.

3. Front-Door Access and Its Limitations

If the measures described in the preceding Section are effective, they may help to push the intelligence community to seek access through the front door. In the next Section, we will analyze to what extent the U.S. government may compel web services to assist law enforcement and intelligence agencies in gaining access to secure communications and what this implies about the efficacy of technical countermeasures such as encryption. More generally, it is important to note that there are multiple ways to gain lawful access to information in the cloud and no clear legal rules with respect to which entity should be targeted (the clouds service, the cloud customer, or the communications infrastructure that is used to connect users and servers). In the absence of such rules, cloud services may rely on technical and organizational measures to dissuade government agencies from targeting the communications infrastructure in favor of a more direct approach to the cloud service or the cloud customer. There are two clear reasons for industry to have a strong preference against access through infrastructure not under its control. First, it negatively affects the relationship with their customers if third parties can gain access to data without the service provider's knowledge and makes it hard to give guarantees about potential access to data by third parties. Second, it would mean that sensitive or valuable business data is accessible to others in the value chain, who could try to use such access for competitive reasons.

But while backdoor access is problematic from the industry's perspective, even front-door access is not wholly satisfactory in terms of addressing the concerns of foreign customers of U.S. cloud services. Most importantly, Section 702 of the FAA authorizes front-door access to cloud computing services under rules that offer reduced privacy protections to non-U.S. persons. Once a so-called selector for the acquisition of foreign intelligence information has been internally approved within NSA, "service providers are legally compelled to assist the government by providing the relevant communications."[163] The differences in the safeguards applicable to U.S. persons and non-U.S. persons under the Section 702 program have been well-documented.[164] Crucially, the Fourth Amendment does not apply to non-U.S. persons outside the U.S., which is clearly reflected in the language of Section 702 itself.[165]

---

163. *See* NSA FISA REPORT *supra* note 15, at 5 (The "tasking under this authority takes place with the knowledge of the service providers.").

164. *See, e.g.*, REPORT ON THE FINDINGS BY THE EU CO-CHAIRS OF THE AD HOC EU-US WORKING GROUP ON DATA PROTECTION (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf (commenting on differences such as a lower threshold for collecting of "foreign intelligence" data; lack of targeting and minimization procedures with regard to overseas collection of data of non-US persons; and lack of Fourth Amendment protection). *See also* LIBE COMMITTEE DRAFT REPORT, supra note 17.

165. *See, e.g.*, REVIEW GROUP REPORT, *supra* note 11, at 153 (noting that "[i]f section 702 were designed to intercept the communications of United States persons, it would clearly violate the Fourth Amendment"). After analyzing Section 702, the Report concludes that "the United States should grant greater privacy protection to non-United States persons than we do today." *Id.* at 131. *See also generally* United States v. Verdugo-Urquidez, 494 U.S. 259, 265-66 (1990).

It follows that foreign cloud customers, even after being reassured about enhanced security against backdoor access to data, may still not find the shift to cloud computing very attractive, given that they do not have access to optimal protection due to current market conditions and offerings. It seems likely that as a result of the transition to cloud computing, the storage and processing of digital information will end up being handled by a relatively small number of players. Eventually, it is this market concentration that could make cloud providers a particularly attractive avenue for government surveillance. But when data of a U.S. or non-U.S. cloud customer is sought from a cloud provider under Section 702 or similar programs, it raises the possibility that foreign intelligence agencies may gain access to the data of foreigners without their knowledge. This represents a significant change in the status quo that organizational customers of cloud services may be unwilling to accept. As mentioned, Microsoft recently asserted itself in this debate. Specifically, it has stated the principle that lawful access should not take place through the targeting of cloud providers but through the targeting of the organizations themselves. According to Microsoft, government agencies should "go directly to business customers or government customers for information or data about one of their employees—just as they did before these customers moved to the cloud—without undermining their investigation or national security."[166]

This may seem like a sound principle from the perspective of both cloud providers as well as their customers. Yet it remains to be seen whether government agencies will respect it. Absent special circumstances, such as the journalistic privilege or medical confidentiality, there are few general legal rules restricting lawful access to data being held by third parties. In the absence of legal reforms, however, industry has started to explore the technical and organizational solutions for implementing this principle in practice.

C. Innovations in Cloud Security: Taking Care of New Business

This Section explores a number of more radical and comprehensive security measures in response to government surveillance concerns. These measures differ from those discussed in Part III.B in two important ways: First, whereas Part III.B described techniques for preventing backdoor access, this Section explores techniques that complicate front-door access as well, and, in some cases, make it impossible or infeasible. Second, the measures discussed below embrace the concept of Privacy Enhancing Technologies (PETs).[167]

Claudia Diaz, Omer Tene, and Seda Gürses have recently analyzed a range of PETs "specifically aimed at enabling individuals to engage in online activities *free from surveillance and interference*."[168] They classify PETs into three categories.[169]

---

166. Smith, *supra* note 2.

167. *See* John J. Borking, & Charles D. Raab, *Laws, PETs and Other Technologies for Privacy Protection*, 2001 J. INFO. L. & TECH., no. 1, *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking (defining PETs as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system").

168. Claudia Diaz, Omer Tene, & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L. J. 923, 924 (2013) (emphasis added).

The first category covers PETs that require "active implementation" by a centralized service provider.[170] These PETs consist mainly in sophisticated cryptographic protocols.[171] They offer certain privacy guarantees with respect to user information while blocking the service provider's access to such information. As Diaz points out, however, they only provide value to users to the extent that the provider actively invests in privacy-enhancing architectures that integrate these protocols into the service.[172]

The second category encompasses client-side PETs as unilaterally deployed by the relatively small number of users who are ready, willing, and able to look after their own privacy interests when interacting with service providers.[173] These PETs also include standalone encryption applications (like PGP) as well as browser add-ons that help maintain the confidentiality of web-based communications or permit anonymous access to online services.[174] These tools do not require any implementation by service providers, although service providers have been known to encourage or discourage their use.[175]

PETs in both of these two categories discussed above may involve what many refer to as "end-to-end encryption" solutions because they provide continuous protection of data as it makes its way from end-user to end-user, regardless of the involvement of service providers.[176] In particular, the client-side solutions are designed to allow sender and receiver to rely on an untrusted and potentially adversarial intermediary such as an ISP or a web-based email service.[177] In contrast, SSL/TLS only protects the data in transit between a user and a service provider. Thus, without further measures, the receiving party has access and even the possibility to tamper with a user's data.

A third category discussed by Diaz et al. consists of collaborative applications that dispense with the need for a centralized service provider operating the service or holding a user's data.[178] All three categories are relevant to cloud security, but

---

169. More specifically, Diaz et al. define PETS as "technologies that address the privacy issues raised by mass collection of data and its possible repurposing for conducting surveillance," while restricting "the scope of PETs to technologies designed to provide privacy protection from untrusted and potentially adversarial data controllers." *Id.* at 940.

170. *Id.* at 925.

171. *Id.*

172. *Id.*

173. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1433-36 (2011) (estimating that most PETs have no more than a million users and discussing the reasons for the lack of consumer demand).

174. Diaz et al., *supra* note 168, at 950-53.

175. *See* Zach Miners, *End-To-End Encryption Needs to be Easier for Users Before Facebook Embraces It*, PCWORLD (Mar. 19, 2014, 4:51 AM), http://www.pcworld.com/article/2109582/end-to-end-encryption-needs-to-be-easier-for-users-before-facebook-embraces-it.html (observing that Facebook's reluctance is at least partially based on difficulties created for the user).

176. *Id.*

177. Diaz et al., *supra* note 168, at 950-53.

178. *Id.* at 954 ("Collaborative solutions are particularly important to achieve privacy protection from traffic analysis."). Traffic data includes the time, order, frequency, and volume of communications, as well as the location and identities of the parties engaged in a communication. *See* DIFFIE & LANDAU, *supra* note 57, at 92 (stating that traffic analysis seeks to interpret non-content attributes of communications in order to gain intelligence). Thus, PETs in this third category aim to provide communications anonymity, and the best known example is the Tor network, which has allows millions

the first two categories (alone and in combination) are of particular interest for the purposes of this Article.

1. The Prospect of Active Implementation of PETs by the Cloud Industry

PETs researchers have developed a variety of privacy-preserving technologies based on advanced cryptographic protocols. These protocols allow a service provider to operate a service "that takes as input private user information without the controller [i.e., the service provider] becoming privy to such information."[179] In particular, researchers have designed smart metering systems and pay-as-you-drive tolling systems that meet these requirements.[180] While these systems remain in the design stage or early implementation stage, privacy-preserving identity management systems are available from well-known enterprise software firms such as IBM and Microsoft.[181]

In the context of web-based and cloud services, there are a number of known solutions that can prevent access of service providers to the actual data of their users. Specific examples include private information retrieval, searchable encryption, and Fully Homomorphic Encryption (FHE).[182] Private information retrieval protocols make it possible for a service provider holding a searchable database to allow and respond to queries on this database without gaining access to the queries.[183] Searchable encryption allows a service provider to provide query results on encrypted data under its control while, neither learning the search terms nor the results.[184] Finally, FHE allows general computations over encrypted data.[185] In other words, it allows a service provider to store encrypted data on a server, process this data without decrypting it, and send the encrypted results of any computations to the client for decryption, thereby fully satisfying the privacy needs of cloud customers.[186] Not surprisingly, FHE is sometimes referred to as the Holy Grail of crypto research.[187]

It is important to emphasize that adoption of the solutions discussed remains low even though some of them are ready for use. There are a number of reasons

---

of users to anonymously browse the web and communicate with each other. Diaz et al., *supra* note 168, at 954.

179. Diaz et al., *supra* note 168, at 944.

180. *Id.* at 944-48.

181. *See* Jan Camenisch, et al., *Concepts and Languages for Privacy-Preserving Attribute-Based Authentication*, *in* POLICIES AND RESEARCH IN IDENTITY MANAGEMENT 34-35 (Simone Fischer-Hübner et al., eds., 2013).

182. *See* MARTEN VAN DIJK & ARI JUELS, RSA LAB., ON THE IMPOSSIBILITY OF CRYPTOGRAPHY ALONE FOR PRIVACY-PRESERVING CLOUD COMPUTING, *available at* https://eprint.iacr.org/2010/305.pdf (last visited Mar. 26, 2014).

183. Benny Chor, Oded Goldreich, Eyal Kushilevitz, & Madhu Sudan, *Private Information Retrieval*, 45 J. ACM 965, 966 (1998). These protocols need to be implemented by the service providers themselves.

184. *See* Rafail Ostrovsky & William E. Skeith III, *Private Searching on Streaming Data*, 20 J. CRYPTOLOGY 397, 398, 401-02 (2007).

185. *See* VAN DIJK & JUELS, *supra* note 182; *see also Cloud Security & Cryptography*, MICROSOFT RESEARCH, http://research.microsoft.com/en-us/projects/cryptocloud (last visited May 7, 2014).

186. VAN DIJK & JUELS, *supra* note 182.

187. *Id.*

for this. First, some of these solutions, such as FHE, are at the very early stages of development.[188] If service provision is limited to the mere storage of data in the cloud, it may be technically feasible for the service provider to anticipate and organize for encryption under the control of cloud users. However, if the cloud provider also has to perform processing operations on the encrypted data stored by its customers, the implementation of privacy-preserving PETs in the cloud context is far more challenging and may even be impossible for complex operations.[189]

Second, many cloud providers lack the incentive to adopt and further develop PETs based on advanced cryptographic solutions that would prevent them from having access to user data. The reasons are obvious: many business models in the cloud industry depend on generating revenue based on access to customers' data (e.g., profiling users for purposes of serving them targeted ads).[190] Thus, for many cloud service providers, the costs of implementing these PETs (loss of profits) outweigh the potential benefits (improved security and privacy guarantees for their customers).[191] Arguably, the new emphasis on security and privacy in the cloud in response to the Snowden revelations might incentivize industry to consider developing and adopting similar measures. Notwithstanding the current lack of adoption, the point this Article seeks to emphasize is that if service providers were to deploy such measures, it would interfere with lawful access requests to cloud providers in some obvious ways. For example, a provider might simply be unable to share unencrypted customer data with law enforcement or intelligence agencies notwithstanding a lawful request for such access.[192]

2. Client-Side PETs and the Cloud: Perfection, Usability, and Uptake

A second category of PETs offers client-side solutions that are deployed by users unilaterally to enhance their privacy while interacting with a central service provider. This category includes various confidentiality tools for content that is hosted or shared through a third-party service. For example, Mymail-Crypt, which

---

188. *See* VINOD VAIKUNTANATHAN, UNIV. OF TORONTO, COMPUTING BLINDFOLDED: NEW DEVELOPMENTS IN FULLY HOMOMORPHIC ENCRYPTION 1-3, http://www.cs.toronto.edu/~vinodv/FHE-focs-survey.pdf (last visited May 7, 2014).

189. VAN DIJK & JUELS, *supra* note 182 (describing the limitations of cryptography alone in ensuring that cloud providers will protect the privacy of users by neither leaking their data nor using it in themselves in an inappropriate manner). One direction in which industry is likely to innovate further is in offering technical architectures for organizational cloud customers that would allow them to set policies for the use and access to data stored and processed in the cloud on their behalf. The idea behind such architectures is that they would enforce certain information privacy and security characteristics by "binding" policies to data through the use of metadata-based architectures, which would subsequently ensure that these policies dictate what can (or cannot) happen to the data in terms of access and processing. For a detailed discussion, see Carolyn Nguyen et al., *A User-Centered Approach to the Data Dilemma: Context, Architecture, and Policy*, *in* DIGITAL ENLIGHTENMENT YEARBOOK 227-42 (M. Hildebrandt et al., eds., 2013). Similar architectures that enable significantly more control over the use and access to data in a cloud environment have been proposed as a way forward in the context of W3C. *See, e.g.*, ALISSA COOPER & CULLEN JENNINGS, CISCO SYS., THE TRUST-TO-TRUST MODEL OF CLOUD SERVICES (Jan. 15, 2014), https://www.w3.org/2014/strint/papers/30.pdf.

190. *See, e.g.*, Soghoian, *supra* note 137, at 378.

191. *See* Rubinstein, *supra* note 173, at 1417-18. These costs do not include the additional costs and complexity of implementing some of these advanced protocols.

192. *See also infra* note 271 and accompanying text.

implements GnuPGP for Gmail, allows Gmail users to encrypt and sign their email.[193] Similarly, Scramble!, which is a Firefox browser extension, allows users to share encrypted messages through Facebook without giving Facebook access to their data.[194] In addition, there are several chat clients that integrate Off-the-Record (OTR) protocols, which provide strong encryption for instant messaging applications.[195] All of these client-side solutions allow users to ensure that non-unauthorized parties cannot gain access to their data or communications when using a third-party service. In addition, they "provide protection from surveillance by the [service provider] itself, who is no longer privy to content communicated by a user."[196]

What happens if the government serves a lawful request for the content of communications on a service provider whose customers utilize a client-side PET for encrypted email or chat? At best, the service providers may hand over encrypted data but these PETs prevent it from furnishing unencrypted data. On the other hand, the provider may fully comply with requests for traffic data unless the user combines a client-side PET with a collaborative PET like Tor.[197]

Cloud providers' attitudes to these client-side PETs are likely to remain ambivalent. On the one hand, they may decide to block their use because they interfere with their business model and desired uses of the service;[198] on the other hand, they may embrace PETs as proof of their good faith efforts to ensure customer privacy in the cloud. By pointing out the possibility to adopt end-to-end encryption solutions, companies could reassure users who are rightly worried about the surveillance of their communications.[199]

Although the availability of encryption solutions may seem attractive for users, they come with some well-documented downsides in terms of usability.[200] As a result, only dedicated or expert users tend to take advantage of them. In fact this is another oft-cited reason for industry to shy away from promoting client-side encryption solutions. In addition, the client-side approach to security tends to rely

---

193. *My-Mail Crypt for Gmail*, CHROME WEB STORE, https://chrome.google.com/webstore/detail/mymail-crypt-for-gmail/jcaobjhdnlpmopmjhijplpjhlplfkhba?hl=en-US (last visited Mar. 26, 2014)

194. Filipe Beato et al., *Scramble! Your Social Network Data*, *in* PRIVACY ENHANCING TECHNOLOGIES 211, 212 (Simone Fischer-Hübner & Nicholas Hopper eds., 2011).

195. Diaz et al., *supra* note 168, at 950-51, ("(OTR) protocols, provide content confidentiality, perfect forward secrecy, and repudiability . . ."); *id.* at 951 (noting that Adium, Cryptocaty, Xabber, and IM+ are a few examples of open source implementations of OTR protocols that work with instant messaging clients).

196. *Id.* at 951.

197. In such cases, the service provider would have difficulty complying with a "pen register" order as well. *See infra* note 264 and accompanying text.

198. *See, e.g.*, Ben Woods, *Mobile Operators Confirm Tor Block*, ZDNET (Jan. 24, 2012, 16:38 GMT), http://www.zdnet.com/mobile-operators-confirm-tor-block-4010025282.

199. *See, e.g.*, Miners, *supra* note 175 (citing Facebook's Chief Security Officer Sullivan as suggesting that "[i]f Facebook users want that type of security, there are some third-party apps they can use to add end-to-end encryption to Facebook's services," and stating that "[a]t a minimum, we want to support third-party initiatives").

200. Usability is a major issue in the uptake and appropriate use of more secure services. *See, e.g.*, ALMA WHITTEN & J.D. TYGAR, WHY JOHNNY CAN'T ENCRYPT: A USABILITY EVALUATION OF PGP 5.0, *available at* http://www.gaudior.net/alma/johnny.pdf (last visited Apr. 4, 2014); *see also* Miners, *supra* note 175.

on the free or open source software model, in which developers release their source code, thereby allowing the security community to review the code and determine that the software is indeed secure. From an ordinary user's perspective, this substitutes trust in a group of security experts in lieu of trusting the third-party services. Finally, it is true that the implementation of end-to-end encryption may help to protect against third party access to raw data through the service provider. From the perspective of managing information security more generally, however, many organizations and individuals may prefer trusting a dedicated service provider over having to rely on their own expertise.

Of course, the Snowden revelations may boost the adoption of end-to-end encryption as a way of limiting the widely publicized systematic monitoring of global Internet communications. Certainly, the NSA's targeting of major cloud service providers through programs like PRISM has spiked interest in end-to-end encryption solutions, at least according to all the hoopla in the in the popular press.[201] For the moment, however, there seems to be only a small niche market for services that cater to the demand for properly implemented end-to-end security, as evidenced by services such as Lavabit,[202] Hushmail,[203] Silent Circle,[204] and Heml.is.[205]

The Lavabit webmail service is an especially interesting example because of its ongoing legal battle with the U.S. Department of Justice (DOJ). Lavabit sought to provide encrypted email services, while resolving the usability issues typical of client-side solutions.[206] The design involved a public-private key infrastructure managed by Lavabit.[207] As usual, each user was assigned a public key and a private key.[208] Whereas decentralized encrypted email standards such as OpenPGP require users to manage keys themselves,[209] Lavabit stored and organized the encryption keys on behalf of its users.[210] To prevent itself from having access to the private keys of its users, Lavabit encrypted the private key with a password known only to the user, which it did not store on its servers.[211] In other words, Lavabit allowed the user to log into the service over an encrypted SSL/TLS connection with a

---

201. *See supra* note 4.

202. Lavabit is an encrypted mails service which shut down in response to demands to hand over customer data to federal prosecutors. *See infra* notes 206-213 and accompanying text.

203. *About*, HUSHMAIL, https://www.hushmail.com/about (last visited Apr. 4, 2014) (describing Hushmail as "a privacy-oriented email service with built-in encryption and no third-party advertising.").

204. *About Us*, SILENT CIRCLE, https://silentcircle.com/web/aboutus(last visited Apr. 4, 2014) ("[A] revolutionary peer-to-peer global platform of encrypted services for mobile devices that enable private and secure voice, video, text and file transfer services.").

205. HEML.IS, https://heml.is (last visited May 7, 2014); *see also* Siraj Datoo, *Pirate Bay Co-founder to Release Hemlis Encrypted Messaging App*, THE GUARDIAN, Jul. 10, 2013, 7:48 EDT, http://www.theguardian.com/technology/2013/jul/10/pirate-bay-hemlis-encrypted-messaging-app-encrypt.

206. For a critical discussion of the design of Lavabit, see Moxie Marlinspike, *A Critique of Lavabit*, THOUGHTCRIME.ORG (Nov. 5, 2013), http://www.thoughtcrime.org/blog/lavabit-critique.

207. *Id.*

208. *Id.*

209. J. Callas et al., *OpenPGP Message Format*, IETF (Nov. 2007), http://www.ietf.org/rfc/rfc4880.txt.

210. Marlinspike, *supra* note 206.

211. *Id.*

normal password and then gave the user access to his or her decrypted email.

As a result of the design and it apparent focus on usability, the Lavabit system had some obvious weaknesses, as compared to powerful adversaries, which have been widely discussed in reaction to the Lavabit court case.[212] In particular, anyone gaining access to the unencrypted communications between a user and the service would be able to retrieve the user's password and decrypt all of the users' email. After law enforcement successfully obtained a court order requiring Lavabit to hand over its private SSL key—thereby giving it access to the user's password—the owner of Lavabit decided to shut down the service in protest.[213] It is to these types of legal conflicts that we turn in the next Section.

IV. CLOSING BACKDOORS AND SHAPING FRONT-DOORS

When looking at the measures discussed in the previous Section, it becomes clear that there are technical possibilities to design cloud services in ways that limit the ability of cloud providers to access the data of their customers. This Article takes the position that the ongoing discussions over cloud security and the increased worries over transnational surveillance are likely to spur further innovation and subsequent adoption of such solutions in the marketplace.

High-security demanding customers such as government agencies and corporate and organizational users with particularly strict demands for information security are likely to drive these market responses.[214] Customers will insist upon better guarantees of security and confidentiality and may refuse to do business with popular, U.S.-based cloud services subject to far-reaching government surveillance powers. Indeed, they may be barred from doing so under new proposals in Europe and elsewhere requiring their citizens to rely on local cloud services.[215] In the market for individual users of cloud resources, there may generally be an increasing demand for better security and privacy safeguards as a result of the widely discussed examples of mass surveillance of online interactions and communication. In addition, law and regulation may increasingly require that certain types of disproportionate lawful access to cloud data be excluded if cloud providers want unrestricted access to the market.

Are these measures likely to be effective against intelligence agencies with the skills and resources of NSA or GCHQ? The answer depends on a variety of factors, which will be discussed further in this Section. One thing is clear: the range of technical solutions described in Part III is not binary, and recent announcements of 'NSA-proof' services seem highly oversimplified.

A better way of framing this topic is to ask a series of more nuanced questions as follows: First, can technological and organizational design of services help to protect against *backdoor* access of data in the cloud? Second, and related, can the

---

212. *See, e.g.*, Larry Seltzer, *Lavabit Security Was a Facade Says Crypto Expert*, ZDNET, (Nov. 7, 2013, 5:00 PST), http://www.zdnet.com/lavabit-security-was-a-facade-says-crypto-expert-7000022919.

213. *See* Spencer Ackerman, *Lavabit Email Service Abruptly Shut Down Citing Government Interference*, THE GUARDIAN, Aug. 9, 2013 2:58 EDT, http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden (noting that Lavabit shut down after refusing to comply with a government surveillance request apparently targeting Edward Snowden).

214. *See also* Van Hoboken et al., *supra* note 2, at 35.

215. *See supra* note 10.

cloud industry help to prevent bulk and dragnet access to the data of their customers? Third, to what extent can the technical and organizational design of cloud services help to shape lawful access dynamics, such as *where* and *how* lawful access takes place (i.e., which entity and in which geographical location)? And, finally, to what extent can government agencies armed with surveillance orders counter the design choices of industry players when new technologies undermine lawful access to data in the cloud the government is seeking?

Based on the analysis outlined herein, the first question should be answered positively. As cloud services roll out new security and encryption measures with the goal of preventing bulk data collection by surreptitious means, this will undoubtedly interfere with large scale intelligence gathering, such as the interception of client-server and server-server data streams. Firms like Google, Microsoft, Yahoo, and Facebook have already begun to implement well-established techniques such as TLS/SSL and perfect forward secrecy, just as various security organizations have begun to review how they develop cryptographic standards.[216] At the end of the day, the protection against backdoor access is also a matter of resources, however. Certain technological solutions may prevent effective bulk collection through specific intelligence programs, but intelligence agencies could in turn deploy targeted intelligence operations to undo some of these protections implemented by cloud services.

The second question, which concerns the possibility of cloud firms preventing dragnet surveillance, cannot generally be answered affirmatively. Technological design may have some impact on front-door collection but where surveillance regimes like Section 702 of the FAA authorize large scale transnational surveillance directed at cloud services, industry has limited options. It may oppose orders in court,[217] or it may take a public stance to the effect that certain types of lawful access should not be legally permissible under current statutes and strive for legal reforms that would enhance the privacy interests of cloud customers.[218]

The third question must be answered positively also, at least in theory. Technological and organizational design of services can help to shape lawful access dynamics and could be used precisely to do so. While few cloud services have actively implemented privacy-preserving encryption protocols, there is reason to believe that this is changing. As discussed in the previous section, both the cloud industry and the Internet security engineering community have taken the first

---

216. *See* William Jackson, *NSA's Reported Tampering Could Change How Crypto Standards are Made*, GCN (Nov. 4, 2013), http://gcn.com/Articles/2013/11/04/NIST-crypto-review.aspx?Page=2; *see also* Dan Goodin, *Stop Using NSA-Influenced Code in Our Products, RSA Tells Customers*, ARS TECHNICA (Sept. 19, 2013, 7:43 PM) http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers.

217. *See* Alex Wilhelm, *Microsoft Is Challenging The US Government's Use Of Search Warrants To Access Data Stored Abroad*, TECHCRUNCH (Apr. 25, 2014), http://techcrunch.com/2014/04/25/microsoft-is-challenging-the-us-governments-use-of-search-warrants-to-access-data-stored-abroad;
Brian Byrne, *Microsoft in Battle with US Government Over Bank Account Info Held in Ireland*, INDEPENDNET.IE (Apr. 28, 2014, 2:30 AM), http://www.independent.ie/business/technology/microsoft-in-battle-with-us-government-over-bank-account-info-held-in-ireland-30223329.html

218. *See* Craig Timberg, *Tech Companies Urge Lawmakers to Reform NSA Programs*, WASH. POST, Oct. 31, 2013, http://www.washingtonpost.com/business/technology/tech-companies-urge-lawmakers-to-reform-nsa-programs/2013/10/31/f100ced6-4264-11e3-a751-f032898f2dbc_story.html.

steps towards implementing technical and organizational measures to shape the lawful access dynamics induced by the use of their services and further innovations may be anticipated. The extent to which local jurisdictions may force multinational cloud service providers to comply with domestic laws notwithstanding these new security measures remains a particularly hotly debated issue.[219]

The fourth question can be rephrased as follows: Where the deployment of cloud services with new and/or improved security or cryptographic features limits or undermines lawful access, do investigative agencies have the legal authority under existing statutes to seek court orders compelling U.S. firms to modify their services or the power to persuade firms to do so in order to facilitate surveillance? More broadly, do U.S. firms (other than telephone carriers subject to CALEA) have a free hand in modifying existing services, or designing new services, to make them more resistant to programs like PRISM? Or may the United States government rely on its surveillance powers to oversee the design of cloud services to ensure that court-ordered access remains achievable as authorized by ECPA and FISA?

All of these questions, especially the fourth question, received some attention in 2007 when reports surfaced that Hushmail, an encrypted email service, had handed over "12 CDs worth of e-mails from three Hushmail accounts" in response to a court order.[220] More recently, press coverage and blogosphere discussion exploded when a federal district court authorized the FBI to install and use a "pen trap" device regarding the email communications of a subscriber of Lavabit's secure and encrypted email service; that subscriber was widely presumed to be Edward Snowden.[221] The unsealed court records indicate that at a meeting in late June between Lavabit's founder, Ladar Levison, and the FBI, Levinson refused to comply with the pen trap order.[222] According to the U.S. Attorney for the Eastern District of Virginia, Neil MacBride, who was present at the meeting, it was not clear whether Levison refused "because it was technically not feasible or difficult, or because it was not consistent with his business practice in providing secure,

---

219. *See* Hoboken et al., *supra* note 2, at 9-10.

220. Ryan Singel, *Encrypted E-Mail Company Hushmail Spills to Feds*, WIRED (Nov. 7, 2007, 3:39 PM) http://www.wired.com/2007/11/encrypted-e-mai (describing how the court order was obtained through a mutual assistance treaty between the U.S. and Canada).

221. *See supra* note 198; *see also* Kevin Poulsen, *Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show*, WIRED (Oct. 2, 2013, 5:27 PM), http://www.wired.com/threatlevel/2013/10/lavabit_unsealed (describing, on the basis of recently unsealed court documents, how Lavabit was served "with a so-called 'pen register' order requiring it to record, and provide the government with, the e-mail 'from' and 'to' lines on every e-mail, as well as the IP address used to access" Snowden's mailbox).

222. *See* Response of the United States in Opposition to Lavabit's Motion to Quash Subpoena and Motion for Unsealing of Sealed Court Records at 5-9, In the Matter of the United States Authorizing the Use of a Pen Register/Trap and Trace Device on an Electronic Email Account, No. 1:13 EC 297 (E.D. Va. 2013); In the Matter of the Search and Seizure of Information Associated with [redacted] that is Stored and Controlled at Premises Controlled by Lavabit LLC, No. 1:13 SW 522 (E.D. Va. 2013), In re Grand Jury Subpoena, No. 13-1 (E.D. Va. 2013), *available at* https://www.documentcloud.org/documents/801182-redacted-pleadings-exhibits-1-23.html (Exhibit 17) [hereinafter U.S. Response Brief].

encrypted e-mail service for his customers."[223] MacBride then filed a motion to compel Lavabit to comply with the pen trap order, which also required that Lavabit provide the government with any technical assistance required to implement the order.[224] Prior to a hearing on this motion, MacBride also (1) filed a motion for civil contempt, requesting that Levison be fined a $1,000 for every day that he refused to comply with the pen trap order; (2) obtained a grand jury subpoena ordering Levinson to testify in front of the grand jury and bring with him the encryption keys; and (3) obtained a search-and-seizure warrant authorizing law enforcement to seize from Lavabit "'all information necessary to decrypt communications sent to or from [the account], including encryption keys and SSL keys,' and 'all information necessary to decrypt data stored in or otherwise associated with [the account].'"[225]

At first, Levinson refused to comply with the pen trap order, arguing that handing over Lavabit's SSL "master key," would give the FBI access to the encrypted communications of all of Lavabit's customers, and not just the target of its investigation.[226] In a letter to the U.S. Attorney, Levinson conceded that "it would be possible to capture the required data ourselves and provide it to the FBI."[227] He then proposed to collect the data manually and send it to the FBI at the end of the 60-day order as well as intermittently as his schedule permitted; the government rejected this offer because it did not provide for real-time transmission of the intercepted data as required by federal law.[228] Finally, after the court issued a contempt order against Levison, he handed over the SSL master key, but suspended operations of Lavabit rather than, as he put it in a message posted to the Lavabit web site, "become complicit in crimes against the American people."[229]

As the sealed pleadings became available,[230] many commentators responded with outrage, characterizing the government's demands for Lavabit's encryption keys as "oppressive and abusive"[231] and a "pathetic tale."[232] In what follows, we

---

223. *See* Michael Phillips & Matt Buchanan, *How Lavabit Melted Down*, THE NEW YORKER, Oct. 7, 2013, http://www.newyorker.com/online/blogs/elements/2013/10/how-lavabit-edward-snowden-email-service-melted-down.html.

224. *See* U.S. Response Brief, *supra* note 222.

225. Phillips & Buchanan, s*upra* note 223 (quoting search-and-seizure warrant)*; see also* U.S. Response Brief, *supra* note 222.

226. Phillips & Buchanan, s*upra* note 223. The SSL "master key" protected customer passwords as they traveled from a customers' computer to the Lavabit servers. Customers had to transmit their passwords to Lavabit in order to log into the service and read their encrypted email. Thus, access to the master key would allow the FBI to unlock the password of every Lavabit customers and gain access to their email. *Id.*

227. U.S. Response Brief, *supra* note 222, at 8.

228. *Id.* Additionally, Levinson sought $2,000 in compensation for implementing the solution and an addition $1,500 if he automated the log collection so as to provide data more frequently. *Id.* The government questioned whether this request for compensation constituted "reasonable expenses" under the statute. *Id.*

229. LAVABIT, http://lavabit.com (last visited Mar. 27, 2014) (letter from Ladar Levison).

230. *See* Plaintiff's Ex.1- 3, United States v. Lavabit, No. 1:13 EC297 (E.D. Va. 2013), *available at* https://www.documentcloud.org/documents/801182-redacted-pleadings-exhibits-1-23.html.

231. Mike Masnick, *Lavabit Case Shows Why We Need Tech Literate Judges*, TECH DIRT (Oct. 16, 2013, 7:40 AM), http://www.techdirt.com/articles/20131015/16391524887/lavabit-case-shows-why-we-need-tech-literate-judges.shtml.

analyze the relevant provision of ECPA and FISA requiring firms like Lavabit to assist the government with the installation of pen trap and other surveillance devices. Next, we compare and contrast these provisions with much broader powers conferred by CALEA, at least as to telecommunications carriers. Finally, we identify some guidelines for interpreting the government's power to compel technical assistance and apply them to a number of cases including Lavabit.

A. Technical Assistance Provisions: Statutory Language and Case Law

There are several provisions in ECPA and FISA requiring firms to provide assistance in connection with court ordered interceptions,[233] authorized requests for the installation of pen registers,[234] and authorized directives for acquisition under Section 702 of the FAA, the FISA amendments.[235] The language in all three of these provisions is very similar. It requires that service providers and certain other entities furnish "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference" with the services that the provider is providing to the targeted individual.[236]

What does "minimum of interference" mean? One of the few relevant cases is a Ninth Circuit decision concluding that the FBI's proposed surveillance of oral communications within an automobile could not be completed with "a minimum of interference" with the in-car system's operation because it required the use of a passive listening feature that would have disabled other system services.[237] While the court declined to say how much interference this Section permitted, it did note

---

232. Scott H. Greenfield, *The Lavabit Brief: Breadth-Taking*, SIMPLE JUSTICE (Oct. 11, 2013), http://blog.simplejustice.us/2013/10/11/the-lavabit-brief-breadth-taking. For a more skeptical view of Lavabit's arguments, see Orin Kerr, *Lavabit Challenges Contempt Order in the Fourth Circuit: An Analysis of Its Arguments*, THE VOLOKH CONSPIRACY (Oct. 11, 2013, 1:29 AM) http://www.volokh.com/2013/10/11/lavabit-challenges-contempt-order; Orin Kerr, *A Few Thoughts on the DOJ Brief in the Lavabit Case*, THE VOLOKH CONSPIRACY (Nov. 14, 2013, 1:25 AM) http://www.volokh.com/2013/11/14/thoughts-doj-brief-lavabits-case. *See also* Ed Felten, *A Court Order is an Insider Attack*, FREEDOM TO TINKER (Oct. 15, 2013), https://freedom-to-tinker.com/blog/felten/a-court-order-is-an-insider-attack.

233. 18 U.S.C. § 2518(4) (2012).

234. *Id.* § 3124(a).

235. 50 U.S.C. § 1881a(h)(1)(A) (2012).

236. The wording of Section 702 is slightly different in that it requires the service provider not act "unobtrusively," but rather "in a manner that will protect the secrecy of the acquisition." *See* 50 U.S.C. § 1881a(h)(1)(A). In addition, all three provisions allow the service provider to seek compensation "for reasonable expenses incurred in providing such facilities or assistance." 18 U.S.C. §§ 2518(4), 3124(c); 50 U.S.C. § 1881a(h)(2). In *United States v. N.Y. Tel. Co.*, the Supreme Court upheld a lower court decision directing a telephone company to assist the government with the installation of a pen register under the All Writs Act, 28 U.S.C. § 1651(a), which confers authority on Article III courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 434 U.S. 159, 172 (1977). The *N.Y. Tel. Co.* case was decided prior to the enactment of ECPA and FISA, but is still cited in later cases for the proposition that the powers conferred by the Act extend, under appropriate circumstances, to third parties "in a position to frustrate the implementation of a court order or the proper administration of justice." *Id.* at 174. For a discussion of other cases that mention the All Writs Act in the context of surveillance orders, see Soghoian, *supra* note 137, at 414-15.

237. In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns, 349 F.3d 1132, 1145 (9th Cir. 2003).

that "'[a] minimum of interference' at least precludes total incapacitation of a service while interception is in progress. Put another way, eavesdropping is not performed with a 'minimum of interference' if a service is *completely* shut down as a result of the surveillance."[238] This is consistent with the general principle that "an intercept order may not impose an undue burden on a company enlisted to aid the government."[239] It also rejected the dissent's alternative reading of 18 U.S.C. § 2518(4), according to which "even the complete shutdown of a service can represent the minimum interference, so long as no lesser amount of interference could satisfy the intercept order."[240]

An analysis of the differences between the technical assistance provisions in ECPA and FISA, on the one hand, and CALEA on the other, lends further support to the Ninth Circuit's view of "minimum of interference" as something (considerably) less than total incapacitation of a service. CALEA's intent was to preserve the ability of law enforcement officials to conduct electronic surveillance involving digital telephony.[241] This law requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that a required level of surveillance capabilities is achieved.[242] Telecommunications providers must be able to isolate and intercept electronic communications and deliver them to law enforcement personnel.[243] CALEA also contains three important limits. First, CALEA does not apply to "information services," such as e-mail and Internet access.[244] Second, carriers are only responsible for decrypting, or ensuring the government's ability to decrypt any communication encrypted by a subscriber or customer, if they provide the encryption service and possess the information necessary to decrypt the communication.[245] Third, carriers must "facilitat[e] authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects . . . the privacy and security of communications and call-identifying information not authorized to be intercepted."[246]

Although this third requirement superficially resembles the "minimum of

---

238. *Id*. at 1145 (emphasis in original).

239. *Id*. at 1148 (citing *N.Y. Tel. Co.*, 434 U.S. at 172). In *N.Y. Tel. Co.*, the Court upheld an order, under the All Writs Act, compelling the phone company to install a pen register where compliance with the order required "minimal effort on the part of the Company and no disruption to its operations." 434 U.S. at 175.

240. In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns, 349 F.3d at 1148. It is not clear if this holding is limited to ECPA and would not apply to a Section 702 order under FISA. For a more pessimistic reading of this case, see Soghoian, *supra* note 137, at 404 ("While the Ninth Circuit's decision protected customer privacy in this particular case, the court left a clear path for compelled assistance with covert surveillance if doing so does not hinder a company's ability to provide service to its customers. If anything, this rather hollow victory for the privacy community was actually a win for the government").

241. *See* H.R. REP. NO. 103-827(I), at 22 (1994) (CALEA was designed to provide "law enforcement no more and no less access to information than it had in the past").

242. 47 U.S.C. § 1002(a) (2012).

243. *Id.*

244. *Id.* § 1002(b)(2)(a). "Information services" are defined at 47 U.S.C. § 1001(6).

245. *Id.* § 1002(b)(3).

246. *Id.* § 1002(a)(4)(A).

interference" condition in ECPA and FISA, in fact, it is radically different. CALEA includes an enforcement provision under which the court issuing a surveillance order may not only direct the carrier to comply with the order but also direct that a provider of support services to the carrier or the manufacturer "furnish forthwith modifications necessary for the carrier to comply."[247] This language is far more expansive than anything in the trio of "technical assistance" provisions examined above. Under CALEA, carriers must design services that both comply with authorized governmental surveillance requests and do so in a manner that avoids disrupting the service, and if they fail to build-in surveillance capabilities of the appropriate kind, a court may order them to modify the service to achieve compliance.[248]

In sharp contrast, information services are not subject to any such obligations under CALEA nor does this law confer any power on courts to order modifications to information services that may be needed to ensure compliance. Do courts enjoy such powers under ECPA or FISA? Presumably, they do not. Both statues are quite specific in their grants of authority and in their description of the conditions under which a provider (including various Internet services) may be asked to provide information, facilities, or technical assistance. While Congress has modified ECPA and FISA several times since enacting CALEA, it has not extended CALEA to information services, nor has it extended 18 U.S.C.§ 2522(a) to entities other than telecommunication carriers regulated by CALEA. In the absence of these affirmative steps, the obligations on Internet firms to provide information, facilities, or technical assistance subject to the "minimum of interference" condition in ECPA and FISA must be distinguishable (and less onerous) than the corresponding obligations of telecommunications carriers under CALEA.[249]

B. Applying the Analysis to Three Scenarios

In light of the analysis in Part IV.A, we may now consider three common scenarios in which the government may demand that a service provider furnish information, facilities, or technical assistance with a minimum of interference to its service. The three scenarios involve: first, services subject to CALEA; second, services outside of CAELA's scope and that may or may not have designed their own technical solutions for complying with surveillance orders; and, third, services not subject to CALEA that encrypt their customers' communications as part of the service. In each case, we try to determine the extent to which a service provider must modify the service, its features, or configuration, in order to comply with an authorized surveillance order under ECPA or FISA.

The first scenario is straightforward: if the service is considered a telecommunications carrier under CALEA, then it must ensure that law enforcement officials can intercept communications on its network. But even CALEA does not authorize law enforcement agencies to require any specific

247. 18 U.S.C. § 2522(a) (2012).

248. *See id.* §§ 2522(a)-(c).

249. This past spring, law enforcement officials revived earlier calls for expanding CALEA to a wider range of Internet services. *See supra* note 92 and accompanying text.

design features or system configurations, nor does it prohibit the adoption of any feature or system configurations; rather, it leaves the design decisions to the discretion of the regulated services.[250] Moreover, CALEA only requires support for decryption where "the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[251] In contrast, the service provider is not responsible for "decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer."[252] If, on the other hand, the service provider is an "information service" and, therefore, not subject to CALEA, then it has no obligation to design surveillance-ready services or to design features and system configurations, or to refrain from offering unbreakable encryption, subject to FBI oversight and approval.[253]

The second scenario is more complicated. If an information service not regulated by CALEA receives an authorized assistance order, and compliance with an assistance order entails minimal effort because the company regularly engages in similar activities on its own network for business purposes (such as routine maintenance, detecting and preventing fraud, security, or dispute resolution), then the company has limited basis to object to furnishing assistance. For example, Google, Microsoft, and Yahoo provide web-based email services to hundreds of millions of customers in multiple countries and languages. Suppose that any of these companies developed a capability to clone customers' mailboxes for troubleshooting or security purposes (i.e., make a complete copy of a live mailbox that is configured in the same way and sends and receives all of the same messages as the original but does not in any way interfere with its functionality). The company receives an order to hand over all email content for a few named accounts and, pursuant to 18 U.S.C. § 2518(4), the FBI seeks its technical assistance in cloning the relevant mailboxes. The company would have little basis for refusing to assist the FBI by cloning the mailboxes for the simple reason that under these circumstances the "minimum of interference" condition is surely met.

Moreover, if the company lacked this capability or refused to develop its own solution, the FBI's first resort would be a court order requiring the service provider to install the FBI's own surveillance tools. Towards the end of the 1990's, the FBI developed a number of such tools including a program code-named Carnivore,[254] which came to light when EarthLink refused to install the device.[255] Carnivore is a "packet-sniffer" (i.e., a program that records and analyzes network traffic) and it could be "configured for full wiretap or pen register mode; in the latter, the data content was 'X-ed' out."[256] In 2000, EarthLink was served with a pen register order and told by the government that it wished to install a device on EarthLink's

250. 47 U.S.C. §§ 1002(b)(1)(A), (B) (2012).

251. *Id.* § 1002(b)(3).

252. *Id.*

253. *See id.* § 1002(b)(2)(a).

254. DIFFIE & LANDAU, *supra* note 57, at 269.

255. *See* Nick Wingfield, Ted Bridis, & Neil King, Jr., *EarthLink Says It Refuses to Install FBI's Carnivore Surveillance Device*, WALL ST. J. (July 14, 2000, 12:01 AM), http://online.wsj.com/news/articles/SB963523417716552926.

256. DIFFIE & LANDAU, *supra* note 57, at 269.

network called "EtherPeek" to carry out the order.[257] The company objected on two grounds: first, that doing so would threaten the privacy of its subscribers (because the device allowed the FBI to view the content and header information for all email messages, which exceeded the terms of the order); and, second, that enabling remote access to its network opened up a security hole that might be exploited by others.[258] EarthLink then designed its own software solution to comply with the order but the government was dissatisfied and sought to install a different program called Carnivore.[259] EarthLink opposed this and went to court, where a federal magistrate ruled against it, forcing EarthLink to install the Carnivore device.[260] At some point, Carnivore disrupted services for EarthLink's customers by crashing its remote access servers;[261] however, the magistrate's decision did not address these facts, nor did it consider the "minimum of interference" requirement under Section 2518(4).[262] According to attorney Robert Corn-Revere, who represented Earthlink in the aforementioned litigation, EarthLink and the government eventually reached "an accommodation in which the device was installed and further assurances were made about network security and about protecting the privacy of subscribers generally."[263]

In short, if a service provider lacks a technical solution to comply with an interception or pen register order to provide the government with requested information, it seems that courts will issue appropriate orders allowing the government to install its own surveillance software inside the service provider's network.[264] As a result, any large service provider with the technical and financial wherewithal to build its own solution has a strong incentive to do so given that (1) it is likely to work better than the FBI's; (2) neither disrupts the service, nor opens a security hole; and (3) minimizes government intrusion on customer privacy.

---

257. *See The Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution, of the H. Comm. On the Judiciary*, 106th Cong., 2nd sess. (Apr. 6, 2000) (statement of Robert Corn-Revere, former Earthlink attorney), *available at* http://commdocs.house.gov/committees/judiciary/hju66503.000/hju66503_0f.htm [hereinafter Testimony of Corn-Revere]. *See also* Ann Harrison, *EarthLink: FBI Won't Monitor Our Network*, COMPUTERWORLD (July 18, 2000, 12:01 AM), http://www.computerworld.com.au/article/5865/earthlink_fbi_won_t_monitor_our_network.

258. *See* Harrison, *supra* note 257.

259. *See* CHARLES P. PFLEEGER & SHARI LAWRENCE, SECURITY IN COMPUTING 599 (3d ed. 2003).

260. *See* Wingfield et. al, *supra* note 255*;* Testimony of Corn-Revere, *supra*, note 257.

261. Wingfield et. al, *supra* note 255 ("The FBI connected Carnivore . . . to EarthLink's remote access servers . . .. But Carnivore wasn't compatible with the operating system software on the remote access servers. So EarthLink had to install an older version of the system software that would work with Carnivore . . .. [This] caused its remote access servers to crash, which in turn knocked out access for a number of its customers").

262. *See* In re United States of America for an Order Authorizing the Installation of a Pen Register & Trap & Trace Device, Cr. No. 99-2713M (C.D. Cal. Feb. 4, 2000) (McMahon, Mag. J.), *available at* http:// www.epic.org/privacy/carnivore/cd_cal_order.html. Although Congress inserted "technical assistance" language into the Wiretap Act in 1970, it did not add this language to the Pen Register Act until 2001, almost seven months after the order in the Earthlink case. *See* Pub. L. 107–56, § 225, 115 Stat. 292, 296 (2001)

263. Testimony of Corn-Revere, *supra* note 257.

264. The FBI eventually re-named Carnivore "DCS 1000" and has continued to invest heavily in improving and expanding this technology. *See* Ryan Singel, *Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates*, WIRED (Aug. 29, 2007), http://www.wired.com/politics/security/news/2007/08/wiretap.

The third, and final, scenario is even more complex because it involves encryption, which is a method for hiding information from unintended recipients including law enforcement and national security. Lavabit is a highly relevant case in point because it illustrates an underlying ambiguity in the "minimum of interference" condition. As previously discussed, Lavabit offered secure email with advanced encryption features.[265] When the government sought information on one of its customers, Lavabit refused to comply. It argued that handing over its SSL master key would expose all of the mail sent or received by its customers to the prying eyes of the government, and therefore violated Lavabit's promise of security via encryption, forcing it to shut down its business entirely.[266] Yet, as Lavabit later confirmed, it could assist the FBI in installing a pen-trap device and providing access to the requested information in unencrypted form without disrupting its service.[267]

This tension between Lavabit's promise of security on the one hand, and its ability to assist the government despite this promise on the other, raises an interesting question with some troubling implications. The question is this: if a firm such as Lavabit designs a secure email service that does not ordinarily enable the government to monitor all of its customers' communications, can the government circumvent this assurance by means of a surveillance order supported by a grand jury subpoena for its encryption keys? Orin Kerr, a leading expert on surveillance law, suggests that Lavabit's claim that its business model somehow trumps the government's power to conduct surveillance authorized by the Pen Register Act is a "really weak argument."[268] As Kerr suggests, it makes little sense to view a subpoena as oppressive or unduly burdensome merely because it allows the government "to conduct the surveillance it is allowed to conduct under the Pen Register statute."[269]

Kerr's view may prevail but it neglects the broader implications of rejecting Lavabit's argument, namely, that it incentivizes services like Lavabit to design secure email systems so that it is not merely burdensome, embarrassing, and economically injurious to comply with surveillance orders but infeasible, in the very strong sense of being technologically impossible to do so. Ed Felten makes this point by comparing a court order to any other "insider attack" (i.e., an attack in which an employee "copies user data and gives it to an outside party") and suggesting that there are good reasons for services like Lavabit to design their systems to protect against such attacks.[270] According to Felten,

In the end, what led to Lavabit's shutdown was not that the company's technology was too resistant to insider attacks, but that it wasn't resistant. . . . Had

---

265. *See supra* notes 221-232.

266. *See* Ackerman, *supra* note 213 and accompanying text.

267. *See* U.S. Response Brief, *supra* note 222 and accompanying text.

268. Orin Kerr, *Lavabit Challenges Contempt Order in the Fourth Circuit: An Analysis of Its Arguments*, THE VOLOKH CONSPIRACY (Oct. 11, 2013, 1:29 AM), http://www.volokh.com/2013/10/11/lavabit-challenges-contempt-order.

269. *Id.* Kerr supports his objection by citing United States v. Calandra, 414 U.S. 338, 345 (1974) for the proposition that "[c]itizens generally are not constitutionally immune from grand jury subpoenas[,]" even though the duty to testify "may on occasion be burdensome and even embarrassing" and "may cause injury to a witness' social and economic status." *Id.*

270. *See* Felten, *surpa* note 232.

Lavabit had in place measures to prevent disclosure of its master key, it would have been unable to comply with the ultimate court order—and it would have also been safe against a rogue employee turning over its master key to bad actors.[271]

However the Lavabit case may be resolved,[272] it sets up the far more difficult question of whether ECPA or FISA authorize a court to order a service provider not only to disclose a master SSL key, even though doing so violates customer assurances and may force it to shut down its service, but also to subvert the design of its service by installing malware on a target's computer.

This may (or may not) be an accurate description of what happened in the Hushmail case.[273] Hushmail secure email service offers its customers two options: a high-security option, which requires that users install and run a Java-based encryption applet and encrypts and decrypts email only on the customer's computer; and a low-security (non-Java) option, which is more convenient but less secure because it handles encryption and decryption on Hushmail's web server.[274] As a result, Hushmail retains the ability to decrypt user's emails when they select the low-security option (via an "insider attack" like that against Lavabit) but no ability to do so when the customer selects the high-security option.[275] Of course, Hushmail's design does not prevent the company from modifying the Java applet so that it captures the user's passphrase and sends it to Hushmail, thereby enabling the company to decrypt the email and share it with a third-party including the government. But it seems unlikely that the company would destroy its own business by subverting its software in this way and subject itself to a likely deceptive practice enforcement action under Section 5 of the FTC Act.[276] Unlike Lavabit, none of the sealed documents in the Hushmail case have been leaked, so less information is available. Also, it is not clear whether the 2007 court order pertained to a high-security or a low-security user; or if Hushmail modified its Java encryption engine; or if, in the interests of full disclosure, it merely pointed out the possibility of doing so.[277] In short, the Hushmail case exemplifies the dilemmas that the government may begin to face if service providers take the next logical step of adding government agencies to their threat models and designing systems that protect against valid court orders. And while the government has prevailed in its efforts to force niche players like Lavabit and Hushmail to capitulate, it may face a much greater challenge if major Internet firms like Microsoft, Google, and Facebook go down this path in response to the Snowden revelations.

---

271. *Id.*

272. As of this writing, the Fourth Circuit has issued an opinion that affirms the lower court decision on procedural grounds. *See* United States v. Lavabit, LLC, 2014 U.S. App. LEXIS 7112, *44-45 (4th Cir. Va. Apr. 16, 2014) (noting that Lavabit waived its appellate arguments by failing to raise them in the district court).

273. *See supra* note 220 and accompanying text.

274. *Id.* For additional technical details, *see* Martin Brinkmann, *Hushmail: Why You Should Run the Java Version*, GHACKS.NET (Aug. 9, 2013), http://www.ghacks.net/2013/08/09/hushmail-why-you-should-run-the-java-version.

275. Brinkmann, *supra* note 274.

276. *See* 15 U.S.C. § 57a(a)(2) (2012).

277. *See* Singel, *supra* note 220 (noting that a savvy user might detect this modification).

V. CONCLUSION

This Article describes and places in a legal perspective the cloud industry's technological responses to the revelations about ongoing transnational surveillance. By focusing on industry responses and exploring the ways in which the technological design of cloud services could further address surveillance concerns, we provide insights into the prospects of these services shaping lawful government access to the cloud. This intersection of service design, on the one hand, and government demands for access to data, on the other hand, signals a dynamic new chapter in the ongoing debate between industry and governments about the possibility and conditions of secure and privacy-friendly information and communications technologies (ICTs) for global markets.

In particular, we have shown that it is helpful to distinguish between front-door and backdoor access to data in the cloud. Our analysis of industry responses has shown the cloud industry is moving quickly to address interception of their customers' data without their knowledge or involvement by adopting technological solutions that limit lawful access (as far as possible) to legal processes directed at the cloud service itself and/or its customers. Many of these measures could have been implemented much earlier on. They are now becoming industry norms. Industry standards like SSL/TLS and HTTPS, together with a new generation of PETs offering "end-to-end" protection, can be effective tools in preventing bulk acquisition through the targeting of the worldwide communications infrastructure.

In short, technologies can help the industry shape lawful access even though they do not change the legal framework, nor do they overcome the lack of progress in reforming existing legal authorities (such as Section 702 of the FAA) to confine lawful access to the front-door of service providers. We expect that this lack of progress—with respect to transnational legal guarantees of privacy and information security, not only in the U.S. but also elsewhere—will be a strong driver for the wider adoption of more robust and comprehensive privacy technologies in the cloud service context. And we argue that under current conditions, the U.S. cloud industry will increasingly rely on technologies to 'regulate' government data access in an effort to enhance the privacy and information security protections of their foreign customers.

This raises the pertinent question of how the U.S. government may respond to increased resilience of cloud services against lawful surveillance. While FISA and ECPA allow government agencies to obtain orders that ensure the cooperation of providers notwithstanding strong technological protections, existing law does not allow for unlimited bargaining room. Most of the services in question are not subject to CALEA obligations and an extension of CALEA seems neither warranted nor politically feasible under present conditions. Moreover, most of these services have responded to the Snowden revelations by implementing stronger privacy protections (and even some advanced cryptographic protocols). No doubt they await the outcome of the ongoing litigation in the Lavabit case, which may clarify the government's power to compel a service to break its security model in response to a valid surveillance order. However, the Lavabit case does not yet present a scenario in which a service's use of advanced cryptography makes it impossible to comply with a surveillance order by furnishing unencrypted data.

A U.S. government win in the Lavabit case may therefore be little more than a pyrrhic victory, for it could simply further incentivize industry to adopt even stronger technological solutions against surveillance, including both actively implemented and client-side encryption protocols preserving privacy in the cloud.