SECTION 702 MALFISANCE

ALEX KIMATA*

The 2016 standoff between Apple and the FBI over the hacking of an iPhone highlighted the often-contentious conflict between privacy and security.[1] *Protecting constitutional privacy rights for citizens while monitoring information to ensure the U.S. remains safe is difficult. Existing constitutional law focuses on the application of the Fourth Amendment to tangible items, such as a house. However, the internet and other forms of digital communication lack the characteristics of tangible objects, and thus existing privacy law may not work. As the ways in which consumers share information shifts from paper and pen to digital technology, the law has had to find the appropriate balance between individual digital privacy and government digital security. Adopted before sensitive digital intelligence information was available, the Foreign Intelligence Surveillance Act (FISA) has had a difficult time finding this balance in this new era of information as well.*

Originally, FISA was created to balance the government's surveillance of security threats and citizens' privacy rights. In 2008, FISA Section 702 was added in an amendment to codify legal grounds for surveillance of non-domestic communication. Although 702's aim is not controversial, both the practical implementation of the program and the National Security Agency's (NSA) legal interpretation of Section 702 have proven to be very controversial. The government has used Section 702 to compel information from telecom and tech companies and to access the emails of millions of people, including Americans. Furthermore, the government's lack of transparency has made it hard for citizens to know which conversations can be monitored and which ones are actually monitored.

Statutory or regulatory changes to FISA have been proposed to resolve this controversy and to ensure that individual privacy rights are adequately protected. However, this is not the only way that change can be effected. This paper suggests three different solutions in the context of FISA Section 702 to

* Alex H. Kimata is a 2018 graduate of the University of Colorado Law School. Alex served as an Article Editor for Volume 16 of the Colorado Technology Law Journal (CTLJ). Alex would like to thank the members of CTLJ for their hard work and comradery which made CTLJ a joy to be a part of. Specifically, he would also like to thank Professor Amy Griffin for all her help with this article and Professor Blake Reid for his guidance and mentorship during law school.

1. Arjun Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 6:34 AM), http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html [https://perma.cc/X9PQ-ZSBE].

ensure that individual privacy safeguards are protected: (1) change the FISA court, (2) strengthen consumer rights, and (3) forge privacy rights by companies.

INTRODUCTION

Today, it is not surprising that privacy and national security interests clash. At its most basic, privacy seeks to keep information private, yet security, especially national security, depends on the opposite—uncovering information so that protective measures can be taken. As information shifts to a digital medium, so has the battle between privacy and national security. Although President Donald Trump has suggested that his solution to this dilemma is to handwrite everything and deliver it by courier,[2] this solution is neither feasible nor practical. Instead, a solution that balances digital privacy and national security is needed.

The Foreign Intelligence Surveillance Act (FISA) was supposed to provide this solution. However, as described below, the application of FISA has failed to provide adequate privacy protections. This paper examines the shortcomings of FISA and advocates for reforms.

In Part I, this paper examines the shortcomings of Section 702 of FISA, by providing the background on how the public became aware of this section of FISA, the negative impact these disclosures had on the public, and how the current implementation of Section 702 of FISA violates the privacy rights of U.S. citizens. Part II examines possible fixes to this problem, focusing on three different solutions: (1)

2. Chris Matyszczyk, *Donald Trump: 'No Computer Is Safe,' So Use a Courier Instead*, CNET (Jan. 1, 2017, 8:28 AM), https://www.cnet.com/news/donald-trump-no-computer-is-safe-use-courier-russian-hacking/ [https://perma.cc/3QGT-BCVV].

changing the way judges overseeing FISA are selected, (2) encouraging private U.S. citizens to strengthen their own privacy rights, and (3) encouraging major technology companies like Google to prioritize privacy rights for their customers.

I. SHORTCOMINGS OF FISA

A. How the Public Learned about FISA

In June 2013, the U.S. population was first made acutely aware of just how expansive the government surveillance program was.[3] Edward Snowden, who was then an unknown former employee of the NSA, secretly met with Washington Post and The Guardian journalists in Hong Kong to discuss the program.[4] On June 5, 2013, The Guardian, published a report stating that, via a court order, the NSA was collecting telephone records from millions of Verizon customers.[5] The following day, the Washington Post published NSA slides that showed a top-secret program named Planning Tool for Resource Integration Synchronization and Management (PRISM).[6] The disclosures revealed that the government used PRISM to compel major technology companies to hand over user data related to foreign communications traffic.[7] The paper alleged that major telecom and tech companies were involved, including Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, and Apple.[8]

However, many companies angrily denied such accusations when contacted by the Washington Post to confirm their participation in the program: "We do not provide any government organization with direct access to Facebook servers," Joe Sullivan, the Chief Security Officer of Facebook responded.[9] Apple said that "[w]e have never heard of PRISM . . . . We do not provide any government with direct access to our servers, and any government agency requesting customer data must get a court order."[10] Google issued a denial stating

3. Barton Gellman, Aaron Blake, & Greg Miller, *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html [https://perma.cc/4C83-N7V5].

4. *Id.*

5. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/4AAG-UE4N].

6. *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ [https://perma.cc/DW3C-55EV].

7. *Id.*

8. *Id.*

9. Chenda Ngak, *Apple, Google, Facebook, Yahoo, Microsoft, Paltalk, AOL Issue Statements of Denial in NSA Data Mining*, CBS NEWS (June 7, 2013, 2:44 PM), http://www.cbsnews.com/news/apple-google-facebook-yahoo-microsoft-paltalk-aol-issue-statements-of-denial-in-nsa-data-mining/ [https://perma.cc/895B-SXQK].

10. Barton Gellman & Laura Poitras, *U.S. British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://

that, "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law . . . but Google does not have a 'back door' for the government to access private user data."[11] Microsoft issued a statement saying that

> we provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition, we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data, we don't participate in it.[12]

Yahoo's denial stated that, "Yahoo! takes users' privacy very seriously . . . [w]e do not provide the government with direct access to our servers, systems, or network."[13]

Two days later, President Obama responded to the reports in a speech that verified the existence of both programs.[14] Obama stated he took seriously his duty to keep the American people safe while also respecting their privacy. "[W]e [were] striking this balance between the need to keep the American people safe and our concerns about privacy, because there are some trade-offs involved," he stated,[15]

> Modest encroachments on privacy that are involved in getting phone numbers or duration without a name attached and not looking at content- that on, you know, net, it was worth us doing. It's important to recognize that you can't have a hundred percent security and also then have a hundred percent privacy and zero inconvenience. You know, we're going to have to make some choices as a society.[16]

Furthermore, President Obama defended the program saying,

> I will leave this office at some point, sometime in the last—next three and a half years, and after that, I will be a private citizen. And I suspect that, on a list of people who might be targeted so

---

www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/3YKN-8SXL].

11. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013, 15:23), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/NB85-KP83].

12. Gellman & Poitras, *supra* note 10.

13. *Id*.

14. President Barack Obama, *Statement by the President*, WHITE HOUSE (June 7, 2013, 9:01 AM), https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president [https://perma.cc/3DUY-TZWU].

15. President Barack Obama, *Obama's Remarks on NSA Controversy*, WALL ST. J. (June 7, 2013), http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/ [https://perma.cc/82FP-YXAP].

16. Obama, *supra* note 14.

> that somebody could read their emails or listen to their phone calls, I'd probably be pretty high on that list. It's not as if I don't have a personal interest in making sure my privacy is protected.[17]

As newspapers continued to investigate government surveillance, the government continued to act in the name of security. The Washington Post published reports that the NSA was "harvesting" hundreds of millions of contact lists from personal e-mail and instant messaging accounts outside of the United States.[18] Because large technology companies, like Google and Facebook, maintain extensive data centers around the world to balance their servers, the NSA was able to collect large amounts of data.[19] The Washington Post also published links disclosing a new program called MUSCULAR, which collected millions of records every day from internal Yahoo and Google networks.[20] The Washington Post disclosed that, in the previous 30 days since its data collection, U.S. surveillance allegedly collected 181,280,466 new records, including metadata recording the sender, recipient, and the content of emails.[21] Surveillance obtained these interactions from looking at undisclosed interception points along fiber optic cables.[22] When the Washington Post contacted the NSA, the NSA reiterated that it was discovering and developing intelligence about valid foreign intelligence targets—"NSA applies attorney general-approved processes to protect the privacy of U.S. persons minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention, and dissemination"[23] In response, Google stated the company has "long been concerned about the possibility of this kind of snooping" and did not provide the government with access to its systems.[24] Yahoo also denied cooperating, stating "we have strict controls in place to protect the security of our data center, and we have not given access to our data centers to the NSA or to any other government agency."[25]

---

17. *Id*.

18. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?utm_term=.904188b70c19 [https://perma.cc/3YZ6-L2G5].

19. *Id*.

20. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), https://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 [https://perma.cc/9E28-DYMM].

21. *Id*.

22. *Id*.

23. *Id*.

24. *Id*.

25. *Id*.

As more evidence is uncovered, it is becoming clearer that these blanket denials by the technology companies are false.[26] In some cases, it appears the government actively mandated that companies not disclose the program.[27] However, this fails to explain why the companies maintained such strong denials, instead of merely offering blanket statements regarding their inability to talk about national security. In other instances, data has emerged that suggests the companies not only complied with government orders but facilitated processes and technology to make government surveillance easier than required by law.[28] These processes included the creation of separate systems that the government had access to and processes that expedited governmental requests.[29]

B. The Impact of the Disclosures on PRISM Companies and the Public

The public and legal impact of these disclosures illustrates just how seriously consumers take their privacy rights. The disclosures have had a serious impact on both consumer expectations of privacy and the U.S. economy. In particular, the disclosures forced PRISM companies to begin to take action to assuage their customer's fears. Facebook and Microsoft both lobbied and eventually disclosed the total number of government requests they received (although these were total numbers and not reserved just for FISA requests). Facebook disclosed that it received between 9,000 and 10,000 requests in the second-half of 2012.[30] Microsoft later revealed it received between 6,000 and 7,000 requests for data in the second-half of the year.[31] Facebook disclosed that it received between 18,000 to 19,000 requests in the second-half of 2012.[32] Google refused to release numbers, arguing that blanket number requests lose value without an

26. Alexis Kleinman, *NSA: Tech Companies Knew about PRISM the Whole Time*, HUFFINGTON POST (Mar. 20, 2014), http://www.huffingtonpost.com/2014/03/20/nsa-prism-tech-companies_n_4999378.html [https://perma.cc/7WEV-W2MY].

27. Grace Wyler, *All the PRISM Data the Tech Giants Have Been Allowed to Disclose So Far*, MOTHERBOARD (June 19, 2013, 12:40 PM), https://motherboard.vice.com/en_us/article/all-the-prism-data-the-tech-giants-have-been-allowed-to-disclose-so-far [https://perma.cc/G72S-QCPC].

28. Connor Simpson, *How Google and Facebook May Help with the NSA and PRISM*, THE ATLANTIC (June 8, 2013), http://www.theatlantic.com/technology/archive/2013/06/how-google-and-facebook-cooperated-nsa-and-prism/314459/ [https://perma.cc/84F3-BLNP].

29. *Id*.

30. Ted Ullyot, *Facebook Releases Data, Including All National Security Requests*, FACEBOOK (June 14, 2013), http://newsroom.fb.com/news/2013/06/facebook-releases-data-including-all-national-security-requests/ [https://perma.cc/A4WM-H9M2].

31. *Microsoft's U.S. Law Enforcement and National Security Requests for Last Half of 2012*, MICROSOFT (June 14, 2013), http://blogs.microsoft.com/on-the-issues/2013/06/14/microsofts-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012/#sm.000xd0urq10zgex9v2z2fskr3yxdi [https://perma.cc/92P8-MHWV].

32. Ullyot, *supra* note 30.

explanation of what type of government request they responded to.[33] Twitter later published a statement in support of Google.[34] Google, along with Microsoft, later sued the federal government for the right to publish this information.[35]

Google's point is valid. Companies had previously published figures of the number of requests they received from the government but had to exclude the number under FISA as it was a secret program. Without this context, any such publications were not even newsworthy. Within the year, the government recognized the potential problems with the current disclosure rules and for the first time changed its policy to allow PRISM companies to disclose just how many PRISM requests they received each month.[36] Still, these figures were not unrestricted as many privacy activists had hoped; instead, they were a compromise. Companies were only allowed to release ranges instead of precise numbers of requests, and they were not permitted to discuss the details of the requests or the identities of the users involved.[37] Furthermore, as part of the compromise, Google, Facebook, and several other tech companies dropped their suit, seeking the ability to publish more information.[38]

The published data showed that PRISM requests were not isolated to a few requests per year. Google data showed it received fewer than 1,000 requests between July and December of 2012, which covered between 12,000 and 12,999 accounts.[39] From January to June 2013 it received under 1,000 requests affecting between 9,000 and 9,999 accounts.[40] During this same time period, Yahoo received between 30,000 to 30,999 requests, and Facebook received requests covering between 5,000 and 5,999 accounts.[41]

Although it is hard to determine just how large an impact these revelations had on people's privacy expectations, the available data suggested the impact was significant. In 2013, the Wall Street Journal reported that AT&T's desired acquisition of Vodafone was being

33. Motion for Declaratory Judgement, Google v. U.S., https://assets.documentcloud.org/documents/716102/google-foreign-intelligence-surveillance-court.pdf (last visited June 14, 2018) [https://perma.cc/N67V-U588].

34. Dieter Bohn, *Google Opts Out of FISA Disclosure Deal Made by Facebook and Microsoft, Calls It 'A Step Back for Users;' Twitter Agrees,* THE VERGE (June 15, 2013, 12:24 A.M.), https://www.theverge.com/2013/6/15/4432368/google-opts-out-of-fisa-disclosure-deal-made-by-facebook-and [https://perma.cc/H3KF-V6JL].

35. Rory Carroll, *Microsoft and Google to Sue Over US Surveillance Requests*, THE GUARDIAN (Aug. 30, 2013, 20:28), www.theguardian.com/law/2013/aug/31/microsoft-google-sue-us-fisa [https://perma.cc/T7LN-AMZX].

36. James O'Toole, *Requests*, CNN (Feb. 3, 2014), http://money.cnn.com/2014/02/03/technology/security/fisa-data/ [https://perma.cc/DV6Q-RET3].

37. *Id.*

38. Richi Jennings, *Closely Examined IT Companies Disclose FISA Requests*, COMPUTERWORLD (Feb. 4, 2014, 6:41 AM), http://www.computerworld.com/article/2475737/it-management/closely-examined-it-companies-disclose-fisa-requests.html [https://perma.cc/5Y5F-LPWW].

39. O'Toole, *supra* note 36.

40. *Id.*

41. *Id.*

scrutinized because of AT&T's interactions with NSA surveillance programs.[42] Specifically, European officials were worried about entangling their communications with USA governmental surveillance.[43] That same year, Cisco systems reported a sales slump of twelve percent in international orders, including twenty-five percent in Brazil and thirty percent in Russia.[44] In fact, Cisco's sales were expected to decrease by ten percent for the quarter.[45] This was due to a report in which the National Institute of Standards and Technology[46] had told companies that Cisco's cryptographic standards may have been undermined by NSA surveillance.[47] Additionally, these revelations spurred Norway and Brazil to reject U.S. cloud based providers and start building their own services.[48] Indeed, many competitive foreign companies started marking their products as "NSA proof."[49] In all, it is estimated that this disclosure cost the US economy $180 billion by 2016.[50]

All of this might be concerning but excusable if it were contemplated as part of FISA Section 702. However, Section 702, which provides legal justification for many of these programs, is only supposed to target foreign surveillance.[51] Congress specifically contemplated as much in discussions about FISA, and this discussion is reflected in the structure of FISA; Section 702 concerns foreign surveillance whereas Sections 703 and 704 specifically contemplate domestic surveillance (and contain much more stringent surveillance requirements to ensure compliance with constitutional protections for persons in the U.S.).[52]

---

42. Anton Troianovski, Thomas Gryta, & Sam Schechner, *NSA Fallout Thwarts AT&T*, WALL ST. J. (Oct. 30, 2013, 7:32 PM), http://www.wsj.com/articles/SB10001424052702304073204579167873091999730 [https://perma.cc/PF2B-HXMS].

43. *Id.*

44. Richard Waters, *Cisco Cites Emerging Markets Backlash on NSA Leaks for Sales Slump*, FIN. TIMES (Nov. 13, 2013), https://www.ft.com/content/445c67ce-4cb1-11e3-958f-00144feabdc0 [https://perma.cc/8XKD-6CDR].

45. *Id.*

46. Jeff Larson, *NIST to Review Standards After Cryptographers Cry Foul Over NSA Meddling*, PROPUBLICA (Nov. 4, 2013, 3:05 PM), https://www.propublica.org/article/nist-to-review-standards-after-cryptographers-cry-foul-over-nsa-meddling [https://perma.cc/6YRY-8JQG].

47. Trevor Timm, *How NSA Mass Surveillance is Hurting the U.S. Economy*, ELEC. FRONTIER FOUND. (Nov. 25, 2013), https://www.eff.org/deeplinks/2013/11/how-nsa-mass-surveillance-hurting-us-economy [https://perma.cc/HJY8-X4S4].

48. Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, GEO. LAW CTR. (2015), http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2469&context=facpub [https://perma.cc/6DS7-DL6L].

49. *Id.*

50. *How NSA Mass Surveillance is Hurting the U.S. Economy*, ELEC. FRONTIER FOUND. (Nov. 25, 2013), https://www.eff.org/deeplinks/2013/11/how-nsa-mass-surveillance-hurting-us-economy [https://perma.cc/HJY8-X4S4].

51. 50 U.S.C. § 1881(a) (2012).

52. Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L & PUB. POL'Y 117 (2015), http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2364&context=facpub [https://perma.cc/6DS7-DL6L].

Therefore, violations of FISA Section 702 do not merely risk violating the public's trust and notions of privacy, but may impinge upon real constitutional concerns regarding privacy.[53] As opposed to the theoretical concerns that some scholars express about other privacy matters,[54] violations of Section 702 have already had real practical impacts on Americans' liberty. Although the NSA is supposed to collect the data to address national security concerns, it has admitted to actively sharing data of Americans with other law enforcement agencies.[55] This policy, called "parallel sharing," is implemented when one agency tips off other law enforcement agencies about a past or future illegal action, and the other law enforcement agency finds a different excuse to uncover the information.[56] This policy exists despite the fact that FISA was supposed to target foreign intelligence only. Furthermore, with regard to defendants, Section 702 requires that each criminal defendant be notified when they are monitored. However, up until 2013, no criminal defendant had ever received such notice. After the New York Times reported that the U.S. Department of Justice (DOJ) had misled the Supreme Court[57] and was evading its notice obligations, the government quickly issued five notices in the next six months. However, any hope that the government had turned a corner was quickly dashed. Notices of FISA are still extremely rare, with the Intercept reporting that their review only found 10 people who received notices of 702 surveillance.[58]

As a result, defendants' rights are almost certainly being infringed, but the defendants have no way of knowing about the infringement because they do not receive notice. Because they do not receive notice, there is no way to challenge the secret surveillance in court. And finally, because there is no way to challenge the secret surveillance, there is no way to find out if defendants were entitled to notice in the first place.

This catch-22 directly affects the lives of the defendants. It also speaks to the problems of the FISA Section 702 program and government surveillance programs in general; it is hard to know if the

53. *Id*.

54. For example, using big data in the Internet of Things to invade privacy consumers.

55. Hanni Fakhoury, *DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations*, ELEC. FRONTIER FOUND. (Aug. 6, 2013), https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering [https://perma.cc/LQ9V-LL5S].

56. *E.g.*, *id*.

57. Memorandum & Order, Foreign Intelligence Surveillance Ct., Nov. 6, 2015, https://www.emptywheel.net/wp-content/uploads/2016/04/151106-702-Reauthorization.pdf [https://perma.cc/MBT6-U5ZG].

58. Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, INTERCEPT (Nov. 30, 2017, 8:29 AM), https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ [https://perma.cc/7C2Q-AJLE]; *see also* Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance—Again?*, JUST SECURITY (Dec. 11, 2015, 9:01 AM), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again [https://perma.cc/KW35-YYHW].

government is breaking the law unless you receive notice of the infraction. Without notice, it is impossible to challenge the government action.

C. Permissible and Prohibited Surveillance under FISA

The September 11, 2001 attacks were the beginning of significant changes within FISA. However, it was not the beginning of the Act. The original version of FISA was introduced by Senator Ted Kennedy and signed by President Carter in 1978.[59] It is somewhat ironic that the bill was originally aimed at confronting abuses of power by former president Richard Nixon, who used presidential resources to spy on political groups.[60] FISA became a solution for dealing with the difficult balance between judicial and congressional oversight of government surveillance programs and protection of national security.[61] It provided for judicial oversight (using the Foreign Intelligence Surveillance Court (FISC)) and congressional oversight through briefing.[62] FISA allows for surveillance without a court order for up to a year unless the "surveillance will acquire the contents of any communication to which a United States person is a party."[63]

Judicial approval of surveillance of a United States person is governed by 50 USC § 1801(f), and is required for: (1) acquisition of data of people who are American, who live in the U.S., and have a reasonable expectation of privacy, and who would require a warrant for law enforcement purposes, (2) the data (to or from) a person in the U.S. if the government has not obtained his/her consent, (3) the intentional acquisition of radio communication if both parties live in the U.S. and there is a reasonable expectation of privacy, and (4) anything other than wire or radio communication if there is a reasonable expectation of privacy.[64] What FISA left open was the question of surveillance of data from parties that are both not Americans and not in the U.S. but whose data traveled in the U.S.

Following the September 11 attacks, President Bush authorized the NSA to surveil Americans and others within the United States to search for evidence of terrorism without court-approved warrants.[65] He justified the program as providing the security and flexibility necessary to target and solve threats. The program authorized the NSA to start collection on a wide range of intelligence, including bulk

59. *The Foreign Intelligence Surveillance Act of 1978*, DOJ, https://it.ojp.gov/Privacy Liberty/authorities/statutes/1286 (last visited Feb. 18, 2017) [https://perma.cc/2JC6-SHQS].

60. *Id.*

61. *Id.*

62. *Id.*

63. 50 U.S.C. § 1802 (2012).

64. 50 U.S.C. § 1801 (2012).

65. *See, e.g.*, James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0 [https://perma.cc/M9SV-4PLL].

information of telephony metadata, online metadata, telephony content, and online content.[66] Originally based on three theories (the President's inherent Article II authorities as commander in Chief, the 2001 Authorization for Use of Military Force, and the War Powers resolution),[67] the Office of Legal Counsel initially declared all collection except the internet metadata to be legal.[68]

However, this authorization was met with both legal and public criticism. The program was first disclosed to the public in a December 15, 2005 New York Times article.[69] It was later revealed that the legal underpinnings for the surveillance program were the work of a single lawyer; DOJ later declared that it was inappropriate that the legal justification of the entire program was not fully vetted.[70] Therefore, in an effort to fully comply with both public opinion and legal pressure, the justifications for surveillance began to change.

A temporary legal justification was found in the Protect America Act, which President Bush signed into law in 2007.[71] It removed the warrant requirement for government surveillance of foreign intelligence targets "reasonably believed" to be outside of the United States.[72] Precise evidence of the target outside the U.S. was not required, only reasonable procedures.[73] This act expired early in 2008, but its core values were soon moved into FISA. Congress passed the 2008 amendment to FISA, which added Section 702 to the original statute. FISA Section 702 empowered the Attorney General and Director of National Intelligence to target persons "reasonably believed to be located outside the United States to acquire foreign intelligence information" for a period of up to one year.[74]

Section 702(b) lays out the following limitations on acquiring the intelligence:

> (a) [surveillance] may not intentionally target any person known at the time of acquisition to be located in the United States, (b) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States, (c) may not intentionally

66. REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, OFFS. OF INSPECTORS GENERAL ET AL. (2009), https://oig.justice.gov/reports/2015/2009JointIGReportonthePSP.pdf [https://perma.cc/SJY4-G8JR]; Donohue, *supra* note 52.

67. UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, OFFS. OF INSPECTORS GENERAL ET AL. (2009), https://fas.org/irp/eprint/psp.pdf [https://perma.cc/S7QM-MW2D].

68. *Id*.

69. Risen & Lichtblau, *supra* note 65.

70. UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, *supra* note 67.

71. Protect America Act of 2007, Pub. L. No. 110-55 (2007), https://www.justice.gov/archive/ll/docs/text-of-paa.pdf [https://perma.cc/QA7Y-NAWV].

72. *Id*.

73. *Id*.

74. 50 U.S.C. § 1802 (2018).

> target a United States person reasonably believed to be located outside the United States, (d) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States, and (e) shall be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.[75]

Additionally, Section 702 lays out guidelines and procedures for targeting individuals and complying with the limitations set out in the act. The Attorney General and Director of National Intelligence must adopt targeting and minimization procedures consistent with Section 702.[76] These targeting and minimization procedures must be provided to congressional intelligence committees, the Committees on the Judiciary of the Senate and House of Representatives, and the FISC.[77] Furthermore, the Attorney General must provide the FISC with written certification that procedures are in place for targeting and minimization that complies with the statute.[78]

D. Structural Problems with FISA

Though FISA was intended to be a robust balance and compromise between privacy and security, revelations following Snowden's disclosures portray a program that has outgrown many privacy checks that were placed on it. Two important presumptions the NSA made are that a "person" is a non-U.S. person and that all targets are located outside the country. [79] Thus, without any evidence to the contrary, the NSA generally assumes that all targets are FISA Section 702 applicable. This interpretation promotes an "ignorance is bliss" mentality at best and more likely presents a perverse incentive to avoid verifying the identity and location of any targets.[80] Furthermore, the NSA has adopted procedures that allow analysts to acquire information about communications modes used by targets.[81] A plain reading of the statute only explicitly allows targeting of communications to and from the target as well as information the target holds.[82] Thus, the NSA has had to expand its reading and interpretation beyond the plain meaning of the statute to allows the PRISM and Upstream programs to exist.

---

75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. OFF. OF GENERAL COUNSEL, FISA AMENDMENTS ACT OF 2008: SECTION 702 (2008), ELEC. FRONTIER FOUND. (Dec. 23, 2008), http://Eff.org/files/2014/06/30/fisa_amendments_act_summary_document_1.pdf [https://perma.cc/3E65-L6LM].
80. 50 U.S.C. § 1801(a) (2012).
81. Donohue, *supra* note 52, at 158.
82. 50 U.S.C. § 1801(f) (2012).

According to Laura Donohue, a FISA expert, it is the fault of both Congress and the FISC that overreaches of FISA were permitted.[83] She asserts that enough information was available in Congress for members to make informed decisions about how FISA could theoretically be used; Congress was accurately informed about the program, could have stopped the program, and yet chose to continue it. [84] Thus, either through negligence or lack of sheer courage to take a public stand, Congress failed to fully vet the law before passing it. She also says the FISC also had an opportunity to protect privacy concerns and weigh in on the implications the statute would have on the Fourth Amendment.[85] By 2011, the FISC realized the implications of NSA's interpretation of Section 702. [86] The FISC determined that there was a history of substantial misrepresentations by the NSA within the collection program.[87] It also noted that it was a crime to "engage . . . disclose . . . or use information obtained under color of law by electronic surveillance knowing, or having reason to know that the information was obtained through electronic surveillance not authorized by statute."[88] However, the FISC noted that through the Upstream program, surveillance is exactly what did happen.[89] The FISC found the targeting procedures to be within the law; despite the statute banning the interception of domestic conversations and the NSA's admission that it knowingly intercepts entirely domestic conversations, the FISC determined that the NSA's actions fell within the statute.[90]

Moreover, Section 702 was supposed to address concerns about "reverse targeting" or "backdoor searches."[91] This procedure targets someone outside the U.S. in order to obtain information about someone within the U.S. by using foreign targets as a proxy to circumvent legal protections afforded to those within the U.S. However, changes by the NSA (with FISC approval) allowed the investigation of content previously collected in the PRISM and upstream telephony collection program using the names and identities of U.S. people.[92] Justifying this, the FISC found that "[l]ike all other

83. Donohue, *supra* note 52, at 158-59.
84. Donohue, *supra* note 52, at 158-59.
85. Donohue, *supra* note 52, at 159.
86. Donohue, *supra* note 52, at 159.
87. [Redacted], 2011 WL 10945618 (FISC 2011).
88. *Id*.
89. *Id*.
90. Donohue, *supra* note 52.
91. Jennifer Granick, *Reforming FISA: A Critical Look at the Wyden/Udall Proposal and Foreign Surveillance*, CENTER FOR INTERNET & SOC'Y (Sept. 30, 2013), http://cyberlaw.stanford.edu/publications/reforming-fisa-critical-look-wydenudall-proposal-and-foreign-surveillance [https://perma.cc/9QKW-W666].
92. James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' Emails and Phone Calls*, GUARDIAN (Aug. 9, 2013, 12:08), https://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls [https://perma.cc/3T8T-F7X4].

NSA queries of Section 702 collection, queries using United States-person identities would be limited to those reasonably likely to yield foreign intelligence information."[93]

Thus, in light of the existing programs under Section 702, the way they are being used, the circumvention of American privacy protections that FISA was supposed to protect, and the continuous breakdowns by those institutions that are supposed to check FISA, it is unsurprising that many people have been especially critical of FISA. Congressional senators such as Wyden and Udall have found common ground with academics and interest groups investigating any overreaches of power.[94]

However, many academics and politicians who wish to reform FISA propose changes within the system and statute to reform the law.[95] While these changes would be very important, there are many reasons to be skeptical of their impact. First, this article has already documented the failure of congressional and judicial oversight that was supposed to ensure that such FISA violations did not occur in the first place. The NSA "legally" conducted its current actions with congressional and FISC permission. To expect both Congress and the FISC to therefore change the status quo and rein in the FISA may be naive. Furthermore, there may be less incentive to do so. As earlier described in the article, President Obama raised an interesting point when he stated that he takes FISA quite seriously because he will one day be a private citizen and FISA will therefore apply to him. Unlike Obama, many members of Congress and members of the FISC are likely to keep their jobs in the near future.[96] Therefore, they may have less incentive to ensure that privacy considerations matter, as it is less likely to affect them personally. Similarly, changing FISA from within puts great faith in the notion that Congress and the FISC will appropriately change FISA without input from those it most impacts (U.S. citizens). Changing the statute alone is not enough to solve current problems.

II. SOLUTIONS

Three particularly significant ways to reform FISA are changing court oversight, forging new privacy rights through consumer action,

93. [Redacted], 2011 WL 10945618 (FISC 2011).

94. *See, e.g.*, Ron Wyden, *Wyden and Udall Statement on the Declassification of FISA Court Opinions on Bulk Collection of Phone Data* (Sept. 10, 2013), https://www.wyden.senate.gov/news/press-releases/wyden-and-udall-statement-on-the-declassification-of-fisa-court-opinions-on-bulk-collection-of-phone-data [https://perma.cc/Y9SQ-J8MA]; Donohue, *supra* note 52; Dia Kayyali, *What You Need to Know About the FISA Court—and How It Needs to Change*, ELEC. FRONTIER FOUND. (Aug. 15, 2014), https://www.eff.org/deeplinks/2014/08/what-you-need-know-about-fisa-court-and-how-it-needs-change [https://perma.cc/9NEV-XB5F].

95. *See, e.g.*, Kayyali, *supra* note 94.

96. *Reelection Rates over the Years*, OPEN SECRETS, https://www.opensecrets.org/overview/reelect.php (last visited Mar. 31, 2018) [https://perma.cc/Z6DN-FWF6].

and creating privacy rights through company action. While each of these actions alone will help protect privacy interests under FISA, all three are needed to create significant change.

Changes to the judicial nomination process for the court that oversees FISA may make the judicial process less of a rubber stamp and more transparent, which will allow consumers more information through which they can start to advocate for their rights. As consumers form rights, they can pressure companies to implement more privacy measures. And companies have greater political and economic power to both pressure the government and implement broad reforms which will lead to different court oversight. However, the fact that all of these changes depend on each other helps explain why change is so difficult in the first place: lack of change in one area creates inertia against change in other areas as well.

A. Court Oversight

One of the supposed primary checks on FISA is the court system created by the statute itself. Much like Article III courts ensure that legislation falls within constitutional boundaries, FISA provided for the FISC to help oversee FISA and ensure that government officials did not abuse their power.[97] However, whether the FISC actually provides an actual check for FISA 702 surveillance is debatable.

The FISC was established as part of the original version of FISA in 1978, and its role is to oversee governmental requests for surveillance.[98] The FISC is responsible for conducting hearings and authorizing four traditional FISA activities: (1) electronic surveillance, (2) physical searches, (3) pen/trap surveillance, and (4) compelled production.[99] Additionally, under the 2008 FISA amendment, the FISC is responsible for reviewing the government's targeting and minimization procedures related to programmatic surveillance.[100]

The current FISC consists of eleven judges, three of whom live within twenty miles of the District of Columbia.[101] The Chief Judge of the United States Supreme Court is charged with appointing judges to the FISC without confirmation or oversight by the U.S. Congress.[102] Since FISA was passed, all three chief justices have been appointed by Republican presidents, including the current chief justice, Justice

97. *About the Foreign Intelligence Surveillance Court*, FISC, http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited June 14, 2018) [https://perma.cc/XG87-5JKD].

98. *Id.*

99. *Foreign Intelligence Surveillance Court*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/surveillance/fisa/fisc/ (last visited June 14, 2018) [https://perma.cc/3NL6-E72X].

100. H.R. Res. 6304, 110th Cong. (2008).

101. FISC, *supra* note 97.

102. *Id.*

Roberts.[103] The current appointment process has resulted in a FISC comprised of Republican judges.[104]

The court's most impactful decisions are those that ensure that the NSA's actions comply with both FISA and individual warrant requirements. By statutory design, all warrant hearings in front of the court are conducted *ex parte*.[105] When government lawyers decide that a certain communication needs to be targeted, they can present the case to the court and receive a ruling on the same day.[106] When individuals are targeted, it is unlikely that they will ever learn of the court's decision, as those decisions are not public.[107] When the government is asking another entity, such as Google, to turn over information or surveillance on an individual, it is unlikely that the company will even know it is a party in the hearing until after a decision has been reached.[108]

Some critics believe that this *ex parte* process unbalances court proceedings too far in favor of the government. While some judges on the FISC have agreed and worked to notify the other parties involved while the proceedings are underway,[109] all such efforts by judges have later been reversed upon appeal.[110] Thus, critics of the FISC argue that the combination of *ex parte* proceedings, the secrecy of the FISC, and the lack of diversity among the judges have resulted in very little protection of people's privacy. Indeed, looking at released figures from the court, from 1979 to 2013 a total of 35,529 requests for surveillance were submitted.[111] Of all the requests submitted, five hundred thirty-three were modified under court direction and only twelve were denied.[112] The rest of the requests were approved.[113] Pro-privacy opponents have argued that this makes the court merely a rubber

103. United States Foreign Intelligence Surveillance Court Letter to Patrick Leahy, FISC (July 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/Leahy.pdf [https://perma.cc/K3U4-XY00].

104. CHART OF PAST AND CURRENT MEMBERS OF FISC COURT, FISC (2016), http://www.fisc.uscourts.gov/sites/default/files/FISC%20FISCR%20JUDGES%20May%2020%202016.pdf [https://perma.cc/B4XV-ALCG].

105. *Foreign Intelligence Surveillance Court*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/surveillance/fisa/fisc/ (last visited June 14, 2018) [https://perma.cc/E7FF-FNGN].

106. *Id.*

107. *Id.*

108. *Id.*

109. Tim Cushing, *Unsealed Yahoo/FISA Documents Show NSA Expected Company, FISC Judge to Operate on Zero Information*, TECHDIRT (May 5, 2016, 11:41 AM), https://www.techdirt.com/articles/20160504/08000134343/unsealed-yahoo-fisa-documents-show-nsa-expected-company-fisc-judge-to-operate-zero-information.shtml [https://perma.cc/3RC5-UA9P].

110. *Id.*

111. ELEC. PRIVACY INFO. CTR., *supra* note 105.

112. *Id.*

113. *Foreign Intelligence Surveillance Act Court Orders 1979-2015*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/surveillance/fisa/stats/default.html (last visited Apr. 1, 2018) [https://perma.cc/GL22-V3DQ].

stamp instead of a real check on abuse of power.[114] Proponents of the government argue that the FISC acts as a deterrent, so that the government only brings appropriate requests to begin with.[115]

However, as described above, many of the interpretations by the NSA seem to violate both the spirit and plain letter of FISA. As detailed above, particularly egregious is the FISC's ruling on the collection of domestic data; the FISC recognized that the NSA's collection of domestic collection violated the law, but simply punted on the issue by stating that safety concerns overrode any such considerations. The FISC's responsibility is to ensure that appropriate balancing of security and privacy concerns occurs, so there must be some actual balancing to ensure that the law works. If security always trumps privacy, then FISA runs into the same legal standing problem that prompted the surveillance to be moved to FISA in the first place.[116] Additionally, when a court fails to provide proper oversight of the act, additional constitutional concerns may be raised.

In an environment where the FISC holds enormous power (it has been called "a parallel Supreme Court"),[117] it is important that its decisions rest on appropriate analysis. This is especially important because the procedure of the FISC only allows for the government to present its side. As there is no opposing counsel to examine and point out weaknesses in the government's case, the burden then falls upon the judges to appropriately vet each case. However, the high percentage of approved requests portrays a system that does not appropriately balance this burden. Indeed, the fact that only twelve requests have ever been denied in more than thirty years and over thirty-five thousand requests suggests that the FISC has fallen victim to the government's influence.

Capture is a well-known phenomenon where an agency becomes dominated by the industries it is charged with regulating.[118] Many times it occurs because special interests have a unique ability to dominate an agency while the general public does not. The excessive number of decisions in the government's favor gives the FISC the appearance of capture. However, in the FISC's case, the capture occurs not because any judge has a more specific interest in being on the FISC but rather because the nomination process is insulated. When only the

114. *E.g.*, Dina Temple-Taston, *FISA Court Appears to be Rubber Stamp for Government Requests*, NPR (June 13, 2013), http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests [https://perma.cc/DSH2-CR8F].

115. ACLU v. Clapper, 13CV3994 (S.D.N.Y. 2013), https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf [https://perma.cc/X3NQ-YLKV].

116. *See infra* p. 12 (showing that surveillance powers were originally moved to the FISA to prevent unfettered power to spy without proper checks).

117. Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N. Y. TIMES (July 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html [https://perma.cc/U4AG-G4A5].

118. *Captured Agency*, U.S. LEGAL, https://definitions.uslegal.com/c/captured-agency/ (last visited June 14, 2018) [https://perma.cc/T2Y9-FZ45].

Chief Justice of the Supreme Court may nominate candidates (without advice and confirmation from any other branch or agency) and all chief justices share many of the same ideological parallels (they have all been conservative), there is a real risk that many of the nominees may share similar ideals and perspectives as well. While this "group think" may help the court achieve greater efficiency, considerable evidence suggests this does not promote as much critical thinking as when a group has diverse members.[119] In dealing with important constitutional issues with little oversight, it is essential that the FISC sacrifice some efficiency for critical inquiry.

Promotion of diverse judges should be the goal of the FISC. Indeed, some proposals for increasing diversity are already in place. Senator Blumenthal has proposed that each of the chief judges of the twelve major appeals courts select a district judge. While Justice Roberts could pick a review panel, six other Supreme Court justices would approve it.[120] Another proposal, parallel to that for all federal judges, provides for nomination by the President and approval by the U.S. Senate. Finally, another proposal suggests that congressional leaders pick eight of the Court's members.[121]

None of the proposals is certain to solve the problem. Each of the proposals suggested has strengths and weaknesses. Senator Blumenthal's proposal may indeed provide the most diverse pool of applicants. The chief justices of appellate courts are very likely to have a diverse set of ideals that would presumably be reflected in their appointments. The downside of this arrangement is twofold. First, there is a real fear that the process may also become politicized, and thus judges will not appoint the most qualified candidate, but someone that they like. Secondly, the bigger fear is that the court may end up with such divergent views that it may inhibit the FISC's ability to correctly do its job. If such divergent views exist that each case that comes before the FISC is a judicial battle (instead of only novel or very complex issues), it could slow the FISC's ability to handle its case load. Because of the vital nature the court plays in protecting constitutional

119. Anna Johansson, *Why Workplace Diversity Diminishes Groupthink and How Millennials Are Helping*, FORBES (July 20, 2017, 2:56 PM), https://www.forbes.com/sites/annajohansson/2017/07/20/how-workplace-diversity-diminishes-groupthink-and-how-millennials-are-helping/#5b4dddad4b74 [https://perma.cc/QK2K-HSX4].

120. Charlie Savage, *Robert's Picks Reshaping Secret Surveillance Court*, N.Y. TIMES (July 25, 2013), http://www.nytimes.com/2013/07/26/us/politics/robertss-picks-reshaping-secret-surveillance-court.html?hp&_r=0 [https://perma.cc/5MND-A2X9].

121. It is, however, a positive development that the USA Freedom act, passed in June 2015, allows for amici curiae. These advocates from diverse backgrounds are tasked with helping the "legal argument that advances the protections of individual privacy and civil liberties; information related to intelligence collection or communications technology; or legal arguments or information regarding any other area relevant to the issue presented to the court." David Kravets, *Let the Snooping Resume: Senate Revives Patriot Act Surveillance Measures*, ARSTECHNICA (June 2, 2015, 3:20 PM), http://arstechnica.com/tech-policy/2015/06/let-the-snooping-resume-senate-revives-patriot-surveillance-measures/ [https://perma.cc/T6KP-AXWB]. While this is a positive development, the decision makers still remain the judges. As such, diversifying the bench still should remain a top priority.

rights while balancing national security, this slowdown could lead to dire circumstances (like the inability for the court to hold timely trials when national security is on the line).

The second suggestion might continue the line of concerns that currently surround the court. Nominations by the President are likely to also be extremely partisan, much like the recent nominations of Supreme Court justices. Because the FISA court holds so much power, and because privacy and national security are such controversial issues currently, it is unlikely that this would change for nominations to the FISA Court. Furthermore, as past confirmation hearings have shown, congressional confirmation has ceased to act like a check and instead either acts like mere rubber stamps or a blockade to the entire process.[122] Combined, this process does not seem likely to lead to varied and nuanced judges on the FISA court.

Finally, the last suggestion also has the benefit of encouraging diverse judges on the FISA Court. The feasibility of this approach depends on who the congressional leaders are and how they frame the problem. Essentially, choosing the leaders from both the house and senate to choose four of the members each runs into the concern that if a party controls both houses in Congress and is the same party as the Supreme Court justice, then there still will not be any diversity of ideas. A successful tweak to this idea may be allow both the Democrats and the Republicans from each house of Congress to choose two nominees. This process would lead to consistently varied judges.

A more effective solution for this problem might be to allow the Senate and House panel on foreign intelligence to nominate and affirm the FISA judges. Doing so would have a number of positive benefits. Committee members are likely to be both very familiar with the subject area and the current threats, leading to some familiarity and expertise in determining factors which are important in FISA judges. Also, the committee is bipartisan, leading to a diversity of ideas about which judges to nominate. Finally, because the committees work so closely with each other and all strive for the same goal (protection of foreign security), there may be less needless blocking of other's nominations and nominations are unlikely to be so ideologically divergent from each other that they essentially stall the court and harm national security in the long run.

B. How Consumers Can Create Their Own Privacy Rights

The assumption that legal rights are only exercised after legislation is passed is mistaken; rights are often forged and therefore exercised before the legal recognition of such a right. In fact, the history of many movements in the United States reflects that rights are forged rather than given. As the internet and internet surveillance is relatively

122. Indeed, nomination and confirmation processes often run along party lines.

new, many of the policies and procedures in this field are still settling. Consumers should not assume that the field is well balanced and should instead work to forge their own rights in this area.

Citizens should begin with Article III and state courts by challenging NSA surveillance on constitutional grounds. Courts have previously held that there is a constitutional right to privacy from government searches.[123] However, it has been difficult to challenge FISA due to a Supreme Court holding that calling information, such as the phone number dialed, is beyond Fourth Amendment protection.[124] In *Smith v. Maryland*, the Supreme Court held that because the consumer had voluntarily turned over the information to a third party (the phone company) for billing and collection purposes, consumers had relinquished any right to privacy with respect to the information.[125] Applying this precedent to *Katz v. United States,*[126] courts have held that no one can have an expectation of privacy in records that they have handed over to someone else.[127] The government has successfully argued that this precedent means that because Americans purposely turn over both phone data and internet data to other companies, Americans have given up any right to an expectation of privacy for that data.[128]

There are, however, many reasons to question this expansive understanding of *Smith*. Professor Laura Donohue argues that significant technological and societal changes mean that the intrusiveness of the technology and the resultant harm to U.S. citizens' privacy interests are fundamentally different from the situation the Court confronted in 1979.[129] It is certainly true that society's reliance on and use of telephone and internet (which did not exist in a usable form when *Smith* was decided) has increased exponentially since *Smith* was decided. Therefore, under this theory, *Smith* should no longer be good policy, and government surveillance of today's technology would be over invasive.

Several new cases provide hope in this matter. Under the recently decided *United States v. Jones* in 2012, the Supreme Court held that Fourth Amendment search occurs where there is a trespass plus "an

123. Katz v. United States, 389 U.S. 347 (1967); Hale v. Henkel, 201 U.S. 43 (1906).

124. Smith v. Maryland, 442 U.S. 735 (1979).

125. *Id.*

126. The court held that Fourth Amendment privacy extends to a public phone booth and a search warrant is required to wiretap a phone booth. The court reasoned this was because the Fourth Amendment protects people, not places and so rejected the appellate argument that such a wiretap was not necessary because there had been no physical intrusion into the phone booth.

127. *See Maryland*, 442 U.S. 735 (1979). l

128. *Announce the Publication of Additional Foreign Intelligence Surveillance Court Filings*, DOJ (Apr. 25, 2014), https://www.justice.gov/opa/pr/department-justice-and-office-director-national-intelligence-announce-publication-additional [https://perma.cc/7MAD-PCBZ].

129. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L & PUB. POL'Y 757–900 (2014).

attempt to obtain information."[130] While not yet litigated, such an interpretation applied to online and telephony information could well find that the NSA did indeed pursue a Fourth Amendment search. Because the search was undertaken under Section 702 and without a warrant, such a search could be deemed illegal.

Other cases have challenged the constitutionality of FISA. However, the process has not been easy or quick, and even obtaining standing has proven to be difficult. In October of 2012, attorneys and human rights organizations challenged the legality of the 2008 FISA Amendment.[131] They argued to the Supreme Court that they sustained greater inconveniences because they were forced to secure their communications with parties overseas, which is where the government might target these communications for surveillance. The Supreme Court dismissed the case for lack of standing, stating that the applicants could not prove that the injury was certainly impending; that the injury was traceable to the FISA provision at issue; and that costs plaintiff incurred were traceable to FISA.[132] However, some progress was made, as the Court at that time did not foreclose the possibility that other members who had suffered an actual injury could bring suit.[133]

Standing was briefly obtained on December 16, 2013 in *Klayman v. Obama*.[134] Subscribers of Verizon Wireless brought suit against the NSA, DOJ, Verizon Communications, President Obama, Attorney General Eric Holder, and the Director of the NSA.[135] They alleged that the government conducted a secret and illegal scheme to intercept vast quantities of domestic telephonic communications in violation of section 215 of FISA, which gives the government authority to compel the production of documents in a national security investigation.[136] The D.C. District Court eventually held that the plaintiffs had standing; that the program constituted a search under the Fourth Amendment; and that subscribers were likely to succeed in showing that the government's searches and the NSA's analysis were unreasonable under the Fourth Amendment. The D.C. District Court enjoined the government from continuing to engage in bulk collection of data.[137] However, progress was once again slowed, as the government later appealed the case, and the District of Columbia Circuit Court of Appeals stayed the injunction, holding that the

130. United States v. Jones, 132 S. Ct. 945 (2012).
131. Clapper v. Amnesty Intern. USA, 133 S. Ct. 1138 (2013).
132. *Id.*
133. *Id.*
134. Klayman v. Obama, 957 F. Supp.2d 1 (D.D.C. 2013).
135. *Id.*
136. *Id.*
137. *Id.*

collection of data by the NSA was legal under the Fourth Amendment.[138]

Next, in *ACLU v. Clapper*, the Second Circuit held that the telephone metadata program exceeded the scope of what Congress had authorized and thus violated the Patriot Act.[139] The ACLU had argued on behalf of subscribers to Verizon that the NSA had unconstitutionally invaded their privacy and Fourth Amendment rights by collecting call metadata.[140] The district court originally ruled that there was no reasonable expectation of privacy, finding that *Smith v. Maryland* meant that all the telephone service meta data was unprotected.[141] However, on appeal, the Second Circuit held that FISA did not prohibit judicial review of the program. The Court of Appeals concluded that the collection of telephone metadata was not relevant to authorize counterterrorism investigations, and so the collection of information exceeded authority granted by FISA.[142] The Second Circuit remanded the case back to the district court for proceedings consistent with the opinion.[143]

The Third Circuit finally entertained standing for an injury under 702 FISA in *Schuchardt v. President of the United States*.[144] A lawyer used email services by Google and Yahoo, as well as other search engines online.[145] After finding that his documents may have been surveilled under the PRISM program, he sued the government.[146] The Third Circuit found that his allegations that bank account passwords, financial data, and privileged and confidential communications with his clients may have been illegally surveilled was a particularized enough injury to plead a case for standing.[147] However, the court stopped short of actually finding standing, remanding the case to district court to determine there was enough factual evidence to allow standing in this suit.[148] The case is still pending.[149]

Thus, the progression of cases shows that by continually bringing lawsuits, privacy advocates have made important gains, such as creating standing where previously the courts were reluctant to recognize these rights. Therefore, bringing future cases that

138. Klayman v. Obama, 805 F.3d 1148, (D.C. Cir. 2015) (noting that developments in *Amnesty v. Clapper* have laid precedent for finding that the NSA collection to be legal).
139. ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).
140. *Id*.
141. ACLU v. Clapper, 959 F.Supp.2d 724 (S.D.N.Y. 2013).
142. Clapper, 785 F.3d.
143. *Id*.
144. Schuchardt v. Obama, 839 F.3d 336 (3d Cir. 2016).
145. *Id*.
146. *Id*.
147. *Id*.
148. *Id*.
149. *Id*.; *see also* Wikimedia Foundation v. National Security Agency, 857 F.3d 193 (4th Cir. 2017) (finding that that Wikimedia also plausibly alleged standing for a 4th amendment violation under its 702 FISA activities. The case was remanded for a factual inquiry on if the plaintiffs have standing).

continually challenge the constitutionality of FISA may lead to a creation of new privacy rights.

Another prominent way for consumers to forge policy rights is by pressuring the government and corporations directly. It was through this sort of direct pressure that the government changed its stance on data that companies were allowed to publicly release.[150] Before Edward Snowden's disclosure, tech companies were not allowed to disclose they were involved in FISA Section 702.[151] Only after the extent of the PRISM program was disclosed did consumer pressure on the government really begin.[152] As a result of this pressure, the government changed its rules to permit the acknowledgement of the existence of FISA Section 702 requests by companies and also allowed companies to disseminate information on the number of requests they had received.[153] Similarly, consumer pressure on companies whose participation in the exposure of FISA Section 702 forced companies to start taking consumer privacy seriously. Google responded to consumer pressure by stating it was rushing to encrypt its data centers: "we see these government agencies as among the most skilled players in this game."[154] By 2014, Google had announced that all Gmail communications were encrypted.[155] The government has responded to consumer pressure as well. Attorney General Eric Holder and the Director of National Intelligence released a joint statement saying "the public interest in disclosing [information about FISA] now outweighs the national security concerns that required its classification."[156]

However, there is still work to be done. Pressure can be put on the government and companies to increase the transparency of PRISM requests and show exact or almost exact numbers instead of broad ranges. Furthermore, as of the publication of this article, many other companies have not promised to encrypt their data, including major companies, such as Yahoo. [157] Increased publicity can also be brought to the issue by pressuring the government to post warnings and terms of conditions on sites where users are susceptible to data interception. As a blueprint, this summer, European Parliament's civil liberties

150. Wyler, *supra* note 27.

151. *Id.*

152. Mark Hachman, *Facebook, Microsoft Disclose FISA requests, sort of*, PC WORLD (June 15, 2013, 8:43 AM), http://www.pcworld.com/article/2042125/facebook-microsoft-disclose-fisa-requests-sort-of.html [https://perma.cc/GZ6U-JQYM].

153. O'Toole, *supra* note 36.

154. Gellman & Soltani, *supra* note 18.

155. Nicolas Lidzborski, *Staying at the Forefront of Email Security and Reliability: HTTPS-Only and 99.978 Availability*, GMAIL BLOG (Mar. 20, 2014), https://perma.cc/5GXL-R9SW.

156. Press Release, James Clapper, Director of National Intelligence, and Eric Holder, Attorney General, New Reporting Methods for National Security Orders (Jan. 27, 2014), https://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1004-joint-statement-by-director-of-national-intelligence-james-clapper-and-attorney-general-eric-holder-on-new-reporting-methods-for-national-security-orders [https://perma.cc/QBA7-YMFT].

157. Gellman & Soltani, *supra* note 18.

committee was presented with a proposal to require every American website to send surveillance notices to EU citizens in order to force the U.S. government to reverse course. The notice stated,

> The users should be made aware that the data may be subject to surveillance (under FISA 702) by the U.S. government for any purpose which furthers U.S. foreign policy. A consent requirement will raise EU citizen awareness and favor growth of services solely within EU jurisdiction. This will thus have economic impact on U.S. business and increase pressure on the US government to reach a settlement.[158]

C. Companies Can Protect Privacy Rights by Using Their Influence and Changing Their Terms of Service

The exposure of the FISA Section 702 program has increased the pressure on companies to provide adequate security and privacy measures. What is important now is that companies recognize how important privacy considerations are to consumers and take appropriate measures to protect these interests.

First, companies have a duty (and a self-interest) to make the best possible effort to protect their customer's data. Before Snowden's disclosure, it was especially troubling that companies seemed not only to be giving up customer information upon a valid court order, but in some instances going beyond what the government requested. For example, The New York Times recently disclosed that Yahoo had secretly built a whole system that was not just scanning individual emails upon governmental request but scanning everyone's email.[159] On the other edge of the spectrum are companies like Apple and Twitter. Apple famously refused to jailbreak its phone for the FBI in the San Bernardino shooting case, due to privacy and security considerations. Twitter is notorious for resisting government requests under FISA Section 702 and only giving up the least amount of required information when it is forced to comply.[160] Famously, Twitter refused to set up a locked box system to make government access of data easier.[161]

Insistence on privacy by these companies is not a lost cause. For example, once it was disclosed that Facebook was a participant in the PRISM program, Facebook lobbied the White House, DOJ, and

158. Timm, *supra* note 47.

159. Charlie Savage & Nicole Perlroth, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N. Y. TIMES (Oct. 5, 2016), http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html [https://perma.cc/G3BN-K4MD].

160. Mike Masnick, *More Details on PRISM Revealed: Twitter Deserves Kudos for Refusing to Give In*, TECHDIRT (June 8, 2013, 12:28 PM), https://www.techdirt.com/articles/20130608/09315223373/more-details-prism-revealed-twitter-deserves-kudos-refusing-to-give.shtml [https://perma.cc/L49P-ZS2D].

161. *Id.*

intelligence officials with more than one hundred calls asking for permission to release data. [162] This was an integral part of efforts to pressure the government into transparency. Currently, Twitter is challenging the transparency report in California courts.[163]

Thus, whether motivated by self-interest in keeping their customer base[164] or a real desire to fight for privacy rights, companies now have a real interest in pursuing privacy safeguards against the government. Furthermore, the influence and clout that these companies wield, as evidenced by Facebook's calls to the White House, may lead them to get quicker returns than U.S. citizens undertaking the same endeavors.

Secondly, companies can work to create terms of service that adequately explain the privacy challenges the company faces, the safeguards which exist to protect their information, and the steps actively being taken to protect their data. Such terms of service do not need to be specific and impinge upon national security, but should at least make the customer aware. For example, terms of service need not mention the PRISM program but should state that all information is available to the government upon proper request.

CONCLUSION

FISA was supposed to help protect American citizens by providing appropriate safeguards to balance privacy and government surveillance. As more information has become available about the program, it has become clear that Section 702 favors national security at the expense of privacy for U.S. citizens. This is especially important because Section 702 was specifically contemplated to exclude communication of domestic residents. FISA enacted Section 703 and 704 for domestic surveillance and these sections include stronger limitations on what the government can do so that it complies with constitutional protections afforded to U.S. citizens. Much of the swing in the balance is not the actual statute itself, but the interpretations of the statute by the NSA with the compliance of the FISC. These interpretations have expanded the definition of what falls under Section 702 to include domestic communication, arguably in violation of the law.

---

162. *Facebook, Microsoft Disclose Government Data Requests, but Google Balks*, WALL ST. J. (June 14, 2013, 9:24 PM), http://blogs.wsj.com/digits/2013/06/14/facebook-got-fewer-than-10000-gov-data-requests-in-2nd-half-of-2012/ [https://perma.cc/YZL5-7W2J].

163. Mealey's, *Twitter Asserts Its Right to Challenge FISA Limits on Reporting DOJ Requests*, LEXISNEXIS (Feb. 9, 2016), http://www.lexislegalnews.com/articles/5889/twitter-asserts-its-right-to-challenge-fisa-limits-on-reporting-doj-requests [https://perma.cc/L4UJ-YYUQ].

164. While many may not leave Yahoo entirely, many customers and advocates were upset to learn that their privacy had been breached. *See e.g.*, Andrew Crocker & Mark Rumold, *Yahoo Email Surveillance: The Next Front in the Fight Against Mass Surveillance*, ELEC. FRONTIER FOUND. (Oct. 4, 2016), https://www.eff.org/deeplinks/2016/10/yahoo-email-surveillance-next-front-fight-against-mass-surveillance [https://perma.cc/J3BV-Y6T9].

However, effective reforms can be taken to help ensure that privacy rights are protected. Many have proposed changes to the FISA statute itself to ensure privacy rights are upheld. While this is one way to propel reform, there are other ways that may be even more effective.

First, changing the composition of the FISC is critically important to ensuring that it does an adequate job of balancing constitutional privacy rights against national security. The current composition of the FISC is heavily conservative, and many have argued that this imbalance has led to a "rubber stamp" of NSA policies and search warrants without a proper analysis of whether the actions are legal. Introducing diverse judges from a variety of backgrounds and ideological places will encourage deep analysis that will better prepare FISC to properly balance privacy rights and national security concerns.

Secondly, U.S. citizens can help forge their own consumer rights. First, by engaging in court cases challenging the constitutionality of the use of Section 702 of FISA, citizens can eventually create strong privacy rights that will more effectively challenge the impositions of national security. *Schuchardt* is an example of such gains.[165] Furthermore, citizens can and should pressure government to continually be transparent about its actions and exactly how it is interpreting the statute. Such pressure will lead to more governmental transparency and signal companies that these privacy rights are important for consumers.

Finally, companies themselves can help push for rights. Companies' primary loyalty should be to their consumers, and they should protect the consumers' security accordingly. Companies should not easily acquiesce to government requests for information and should make every effort to fight the government accordingly. Companies, as illustrated by the example of Facebook, have substantial power over policy. They can wield that power to forge new rights and norms on privacy safeguards, and to increase government transparency about any invasions of privacy. Lastly, companies themselves can be transparent by encouraging full terms of service that adequately explain what types of information they will disclose.

By engaging in these changes, there is a chance that real, effective change can occur in a fairly short period of time.

165. Schuchardt v. Obama, 839 F.3d 336 (3d Cir. 2016).