CHAPTER TWO

STANDING, SURVEILLANCE, AND TECHNOLOGY COMPANIES

Article III limits the judicial power of the federal courts to certain "Cases" or "Controversies."[1] This, says the Supreme Court, burdens a plaintiff with proving, at the very least, that she has "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[2] These requirements often set an insurmountably high bar for would-be surveillance plaintiffs, who struggle to prove that they have suffered an "'injury in fact' that is 'certainly impending'" when most of the evidence that would tend to prove that fact is classified.[3]

To understand why standing has proven to be especially thorny in the surveillance context, it may be useful to begin with a brief primer on the Fourth Amendment as it applies to foreign surveillance. The Fourth Amendment does not protect foreigners located abroad and lacking substantial ties to the United States.[4] It does protect a category referred to doctrinally and in this Chapter as "U.S. persons": American citizens located within U.S. borders, American citizens located abroad, and foreign nationals who are on U.S. soil and have "developed sufficient connection" to the United States.[5] There would be no constitutional problem if U.S. persons, who are protected by the Fourth Amendment, never interacted with non-U.S. persons. After all, the government can constitutionally spy on foreigners located abroad without a warrant even when the collection occurs inside the United States and from domestic intermediaries. But the reality is that U.S. persons *do* interact with non-U.S. persons. This, as we'll see, complicates the picture.

Consider this hypothetical. Viktor is a foreign national located in Russia. He is a highly placed administrator within the Russian Federal Security Service and has therefore been targeted by the U.S. government for surveillance. The government targets persons under section 702 of the Foreign Intelligence Surveillance Act[6] (FISA), perhaps the most important statutory authorization for government surveillance today, by "tasking," or targeting for collection, a "selector," or a specific phone

---

[1] U.S. CONST. art. III, § 2.

[2] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (citations omitted).

[3] Jeffrey L. Vagle, Laird v. Tatum *and Article III Standing in Surveillance Cases*, 18 U. PA. J. CONST. L. 1055, 1055 n.1 (2016).

[4] United States v. Verdugo-Urquidez, 494 U.S. 259, 271–72 (1990).

[5] *Id.* at 265; *see also* Elizabeth A. Corradino, Note, *The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far?*, 57 FORDHAM L. REV. 617, 617 (1989).

[6] 50 U.S.C. § 1881 (2012).

number, email address, or other communications facility.[7] This allows the government to intercept all communications "to" or "from" a selector.[8] The government tasks Viktor's Gmail address. Is this constitutional? So far, so good — Viktor is a foreigner, located abroad, and lacking U.S. ties, and thus may be constitutionally targeted even though Google is a domestic electronic service provider. Viktor has recently begun communicating with Jada, an American journalist, about information at his disposal regarding Russian interference in the U.S. election. They exchange highly sensitive information through emails, including information regarding Jada's sources or methods. So what happens to Jada's replies to Viktor?

This is so-called "incidental collection." The government wouldn't be able to target Jada directly under section 702 because Jada is an American citizen entitled to the Fourth Amendment's protections from unreasonable searches and seizures. But the government nonetheless has access to her highly sensitive communications because it is constitutionally targeting her source. Jada strongly suspects, but does not have a way of proving, that her communications may be intercepted, given that Viktor's position in the Russian government makes it highly likely that he is a section 702 target. What rights does Jada have to challenge the collection? This is the question that this Chapter sets out to answer.

And that answer has grave implications. Most obviously, it implicates the privacy rights of Americans who seek to communicate with foreigners in an increasingly connected world, and their ability to vindicate violations of those rights. And it also bears on the ability of civil society to hold the surveillance state accountable. That answer is not just hypothetical: as discussed later on in this Chapter, the government today incidentally collects the communications of a potentially significant number of U.S. persons, a number it refuses to disclose.[9] But the implications don't end there. As a European high court addressing similar issues of individual standing to challenge surveillance laws put it, "where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified."[10]

---

[7] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 133 n.43 (2015).

[8] *Id.*

[9] *See infra* p. 1747.

[10] Zakharov v. Russia, App. No. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, ¶ 171 (Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324 [https://perma.cc/AT9E-9ZA7] (citing Kennedy v. United Kingdom, App. No. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905 ¶ 124 (May 18, 2010), http://hudoc.echr.coe.int/eng?i=001-98473 [https://perma.cc/P4ND-S87D]).

It thus becomes important, for democratic legitimacy if nothing else, to understand precisely *who* may challenge surveillance laws.

A pair of recent decisions set up a dichotomy in the law of standing to bring constitutional challenges of surveillance. In *Clapper v. Amnesty International USA*,[11] the Supreme Court refused to allow a group of human rights lawyers, journalists, and activists to bring a challenge to a surveillance law because they could not show an injury in fact — that is, they could not demonstrate that they suffered actual harm fairly traceable to the statute.[12] But in *In re Directives*,[13] a court allowed Yahoo to assert its users' constitutional rights and found it had standing to challenge a surveillance law.[14] This dichotomy raises the questions: Are technology companies the actors best suited to challenge surveillance laws? Can they always be trusted to do so?

This Chapter argues that the answer to those questions is "no." After summarizing the law of surveillance and standing in section A, this Chapter in section B explains that technology companies are private businesses, and that while they sometimes may be financially incentivized to resist government surveillance, those same incentives might sometimes lead them to acquiesce to it. Even assuming that technology giants' interests are always aligned with those of their users, there is no guarantee that companies will continue to have standing to challenge surveillance laws as technology evolves. Users, section C contends, should be allowed to be their own advocates; the law, argues section D, can and should be reformed to reflect that.

A. The Law of Surveillance and Standing

The most important statutory authority under which the government conducts surveillance today is section 702 of FISA.[15] Section 702, passed in 2008 as part of the FISA Amendments Act,[16] significantly expands traditional FISA to allow surveillance of foreigners located abroad and using domestic electronic service providers.[17] Though this

---

[11] 568 U.S. 398 (2013).

[12] *Id.* at 410–11.

[13] *In re* Directives to Yahoo! Inc., Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01, 2008 WL 10632524 (FISA Ct. Rev. Aug. 22, 2008) [hereinafter *In re Directives*]. A more extensively redacted version of this decision was originally published in the federal reporter. *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008). However, in 2014, the Office of the Director of National Intelligence released a less redacted version on the intelligence community's online communications portal. *See Statement by the Office of the Director of National Intelligence and the U.S. Department of Justice on the Declassification of Documents Related to the Protect America Act Litigation*, IC ON THE RECORD (Sept. 11, 2014), https://icontherecord.tumblr.com/post/97251906083/statement-by-the-office-of-the-director-of [https://perma.cc/FKQ6-JY38].

[14] *In re Directives*, 2008 WL 10632524, at *3–4.

[15] Adam Klein et al., *The "Section 702" Surveillance Program*, CTR. NEW AM. SECURITY (Aug. 4, 2017), https://www.cnas.org/publications/reports/702 [https://perma.cc/SQ3C-APXK].

[16] Pub. L. No. 110-261, 122 Stat. 2436 (codified in scattered sections of 50 U.S.C.).

[17] Klein et al., *supra* note 15.

Chapter focuses on section 702, given the importance of the statute today, it is highly likely that other statutes that present similar questions will come along as technology evolves.

But though most of the examples in this Chapter concern standing to challenge section 702, the standing question is perhaps even more important for a statute that has not yet been passed or actions the government has yet to take. What happens if Congress passes a statute allowing for surveillance of U.S. persons under a constitutionally dubious rationale in a way that ensures the U.S. person never finds out? Who ensures that this law receives review in an adversarial court proceeding? As the following discussion shows, under current law, a technology company may well be the only actor positioned to do so.

1. The Current Statutory Framework. — Congress passed FISA in 1978 in reaction to a congressional investigation that uncovered a history of presidential abuse of warrantless surveillance going back to at least the time of President Franklin Roosevelt's administration and continuing into the Watergate era.[18] Instead of requiring a warrant supported by probable cause to believe the target had committed a crime, FISA allowed the government to get a court order to spy on people located in the United States when it had probable cause to believe they were agents of a foreign power.[19] This framework is known as "traditional FISA." FISA also created the Foreign Intelligence Surveillance Court (FISC) to review the government's surveillance applications, and the Foreign Intelligence Surveillance Court of Review (FISCR) to review the FISC's decisions.[20]

Section 702 grew out of a series of programs that followed the post-9/11 explosion of the surveillance state, which often operated under a patchwork of legal authorities that required the government to "redefin[e]" parts of the traditional FISA statute[21] to continue operating. To solve this problem, Congress passed the Protect America Act[22] (PAA) in 2007.[23] The PAA was the statute at issue in *In re Directives*.[24] When the PAA expired in 2008, Congress passed the FISA Amendments Act, codified in relevant part as section 702, to act as a more permanent fix.[25]

---

18 William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1225–27 (2007).

19 William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1637 (2010).

20 50 U.S.C. §§ 1803(a)-(b), 1881(b)(2)-(3) (2012). The FISC and FISCR are generally regarded as Article III courts, and the FISCR's decisions are reviewable by the Supreme Court. Stephen I. Vladeck, *The FISA Court and Article III*, 72 WASH. & LEE L. REV. 1161, 1165–69 (2015).

21 *See* Donohue, *supra* note 7, at 128; *see also id.* at 126–28.

22 Pub. L. No. 110-55, 121 Stat. 552 (repealed 2008).

23 *See* Donohue, *supra* note 7, at 135–36.

24 No. 08-01, 2008 WL 10632524, at *1 (FISA Ct. Rev. Aug. 22, 2008).

25 Donohue, *supra* note 7, at 137–39.

The PAA, and section 702 after it, differed from traditional FISA in several crucial respects. Instead of requiring the government to seek an individualized court order supported by probable cause that the target was an agent of a foreign power, the statute allowed the government to authorize surveillance on its own so long as the right procedures were in place.[26] The statute also changed the substance of what the government was required to prove — instead of showing that a proposed target was the agent of a foreign power, it now had to show that it had reason to believe the target was located abroad.[27]

Under section 702, the government "adopt[s] targeting and minimization procedures consistent with the statutory requirements."[28] The government then submits to the FISC certifications detailing these procedures and making statutorily required attestations, such as that "a significant purpose of the acquisition is to obtain foreign intelligence information."[29] FISC's role in reviewing these certifications is limited: FISC *must* approve them if the statute's requirements are met.[30] Though the statute prohibits the intentional targeting of U.S. persons except as consistent with traditional FISA,[31] the NSA has interpreted section 702 to allow collection of communications "to" or "from" a target.[32] As described in this Chapter's introduction, that means that when U.S. persons communicate with section 702 targets, the government incidentally collects their communications, leaving them vulnerable to government abuse. In 2009, the FISA court allowed "the FBI to keep and use its own copy of certain raw messages collected under" section 702.[33] "Agents gained the power to search the database using the names of Americans whom they were scrutinizing, including for unrelated criminal investigations, and read any messages by those Americans that were swept up incidentally and without a warrant."[34] In 2011, the FISC also allowed the NSA and CIA to search the incidental collections database,

---

[26] *Id.* at 136, 139.

[27] *Id.*

[28] *Id.* at 139.

[29] *Id.* at 140 (quoting 50 U.S.C. § 1881a(g)(2)(A)(v) (2012)).

[30] *Id.* (citing 50 U.S.C. § 1881(i)(3)(A)).

[31] 50 U.S.C. § 1881b.

[32] *See* Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (Apr. 28, 2017), https://nyti.ms/2qfmHmb [https://perma.cc/82RP-HWX2]. Previously, the government collected information "about" targets as part of its UPSTREAM program, but "about" collection proved to be so legally vulnerable that the NSA ended it early in 2017. *See id.*

[33] CHARLIE SAVAGE, POWER WARS: THE RELENTLESS RISE OF PRESIDENTIAL AUTHORITY AND SECRECY 557 (rev. ed. 2017).

[34] *Id.*

though those agencies needed to have a foreign intelligence purpose when searching.[35]

Though section 702 also directs the government to follow minimization procedures, there's a loophole: when the NSA determines that these incidentally collected communications may contain evidence of an ordinary crime, it may retain and share them with the relevant law enforcement agencies.[36] So to return to our journalist and source: suppose Jada emailed Viktor information about recently leaked, highly classified documents detailing a meeting between a U.S. government official and a Russian spy — Jada is hoping that Viktor will know the identity of the Russian spy. Jada's actions in receiving the leaked documents and transmitting them to a foreigner may constitute a crime.[37] An NSA analyst reviewing these communications may legally decide to retain Jada's emails and transmit them to the relevant law enforcement agency.

There are no available statistics for how many Americans have had their communications incidentally collected under section 702 — the NSA has consistently refused to disclose that number.[38] But we do know that the government targets over 100,000 people for surveillance — meaning that there are 100,000 "Viktors" out there for the "Jadas" of the world to be talking to.[39] And in 2014, the *Washington Post* analyzed a "cache of intercepted conversations [provided by] former NSA contractor Edward Snowden" and found that nine out of ten account holders involved in the conversations were not the intended targets.[40]

So while we don't know the extent of the problem, we do know this: it is real, and the mass of incidentally collected data on U.S. persons lies about like a loaded gun just waiting for the wrong actor to shoot it, resulting in serious government abuse of Americans' privacy rights.

---

[35] *Id.* The FBI also has the power to request that specific foreigners be targeted for surveillance, *id.* at 557–58, raising concerns that it will target foreigners likely to interact with U.S. persons to avoid having to get authorization to spy on those U.S. persons directly.

[36] Robyn Greene, *Incidental Collection Is Extremely Troubling, Regardless of Legality*, JUST SECURITY (Mar. 24, 2017), https://www.justsecurity.org/39226/incidental-collection-extremely-troubling-legality/ [https://perma.cc/2LGM-P7HW].

[37] *See* David Folkenflik, *Q: Could U.S. Prosecute Reporters for Classified Scoops? A: Maybe*, NPR (Mar. 22, 2017, 5:11 AM), https://www.npr.org/sections/thetwo-way/2017/03/22/521009791/q-could-u-s-prosecute-reporters-for-classified-scoops-a-maybe [https://perma.cc/UJ6N-NRXV].

[38] *See* Spencer Ackerman, *NSA: It Would Violate Your Privacy to Say If We Spied on You*, WIRED (June 18, 2012, 6:29 PM), https://www.wired.com/2012/06/nsa-spied/ [https://perma.cc/6ZXF-RHS3].

[39] *See* Greene, *supra* note 36 (hypo adapted).

[40] Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), http://wapo.st/1mVEPXG [https://perma.cc/Z782-WPXY].

Congress recently reauthorized section 702 for another six years.[41] The new bill has been heavily criticized by civil liberties activists for failing to protect Americans whose information has been incidentally collected, and it does not address any of the standing challenges involved in bringing section 702 litigation.[42] In fact, civil liberties advocates have slammed the reauthorization bill for potentially increasing the amount of incidental collections of Americans' communications.[43] It therefore becomes more important to know just who can challenge section 702.

2. Standing and Technology Companies. — In a recent article, Professor Alan Rozenshtein points out an important dichotomy: due to the FISCR's decision in *In re Directives* and the Supreme Court's decision in *Clapper*, technology companies have standing to challenge surveillance laws that individual plaintiffs do not.[44] The reason for this, this section explains, is the difference in the nature of the harms asserted: because the company could assert its burden of compliance as cognizable injury, it attained Article III standing where the users could not.

(a) In re Directives to Yahoo! Inc., Pursuant to Section 105B of the Foreign Intelligence Surveillance Act. — The first case concerned a challenge by Yahoo to directives issued under the PAA targeting foreigners located abroad to gather foreign intelligence.[45] Yahoo refused to comply with the directives.[46] After the FISC ruled against it,[47] Yahoo challenged its decision in front of the FISCR. Yahoo did not argue that the directives violated any of its own rights as an entity; rather, it challenged the directives as illegally violating its users' Fourth Amendment rights.[48] Despite the general rule "that litigants ordinarily cannot bring suit to vindicate the rights of third parties,"[49] the FISCR explained, it is also commonly accepted that Congress, so long as other constitutional

---

41 Dustin Volz, *Senate Passes Bill Renewing Internet Surveillance Program*, REUTERS (Jan. 18, 2018, 12:47 PM), https://www.reuters.com/article/us-usa-congress-surveillance/senate-passes-bill-renewing-internet-surveillance-program-idUSKBN1F72JX [https://perma.cc/CKC2-8FLD].

42 *Id.* The bill requires the FBI to seek a warrant when it wants to access Americans' communications as part of an already-existing criminal investigation that is unrelated to national security, but privacy advocates have criticized this as doing little to protect most Americans. *Id.* For instance, the bill presumably wouldn't protect journalist Jada, as her communications would not implicate an existing criminal investigation and would implicate national security.

43 See Robyn Greene, *Americans Wanted More Privacy Protections. Congress Gave Them Fewer.*, SLATE (Jan. 26, 2018, 7:45 AM), https://slate.com/technology/2018/01/congress-reauthorization-of-section-702-of-the-fisa-is-an-expansion-not-a-reform.html [https://perma.cc/KP2T-LL8M].

44 Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 132 (2018).

45 *In re Directives*, No. 08-01, 2008 WL 10632524, at *1 (FISA Ct. Rev. Aug. 22, 2008).

46 *Id.* at *2.

47 *Id.* Yahoo began compliance on May 12, 2008, though the number of accounts surveilled between then and the date of the FISCR's decision on appeal is classified. *Id.*

48 *Id.* at *3.

49 *Id.* (citing Hinck v. United States, 550 U.S. 501, 510 n.3 (2007); Warth v. Seldin, 422 U.S. 490, 499 (1975)).

standing requirements (injury, causation, and redressability) are satisfied, may allow a party to bring a lawsuit asserting the rights of others.[50]

Writing for the FISCR, Judge Selya[51] wrote that Yahoo "easily exceeds the constitutional threshold for standing."[52] Yahoo was injured because the government's directives burdened it with "facilitat[ing] the government's surveillances *of its customers*."[53] That injury was "obviously and indisputably caused by the government's directives," and the FISCR is able to redress that injury[54] — presumably through invalidating the directives. Thus, the remaining question was whether the PAA authorized the challenge. The PAA specified that a company could challenge a directive's legality in the FISC and appeal to the FISCR.[55] The court found the statute's language to be "broad enough" to permit service provider challenges "regardless of whether the provider or one of its customers suffers the infringement that makes the directive unlawful."[56] Thus, it found, Yahoo had standing to challenge the PAA.[57]

The court then turned to the merits question: whether the PAA violated the Fourth Amendment. Because the PAA has been "applied to [Yahoo] in a specific setting,"[58] the FISCR declined to consider Yahoo's suit as a facial challenge, opting instead to determine whether the PAA was "unconstitutional as implemented here."[59] It found that it was not. The FISCR recognized a "foreign intelligence exception" to the Fourth Amendment's warrant requirement: so long as the surveillance was "undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States," the government did not need a search warrant.[60]

But the directives still needed to clear the Fourth Amendment's reasonableness standard to be constitutional. The court balanced the government's interests against those of "targeted persons."[61] The court found that the targeting procedures were sufficiently narrowly tailored to minimize accidental targeting of unauthorized targets.[62] It then

---

[50] *Id.* (citing *Warth*, 422 U.S. at 501; then citing Bennett v. Spear, 520 U.S. 154, 162 (1997)).

[51] Judge Selya was joined by Senior Judges Winter and Arnold.

[52] *In re Directives*, 2008 WL 10632524, at *3.

[53] *Id.* (emphasis added).

[54] *Id.*

[55] Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 554 (repealed 2008).

[56] *In re Directives*, 2008 WL 10632524, at *3.

[57] *Id.* at *4.

[58] *Id.*

[59] *Id.* at *5.

[60] *Id.*; *see id.* at *5–7. In *United States v. U.S. Dist. Court* (*Keith*), 407 U.S. 297 (1972), the Supreme Court declined to recognize a domestic surveillance exception, *id.* at 321, but explicitly reserved the question of whether a foreign intelligence surveillance exception existed for another day, *id.* at 308–09.

[61] *In re Directives*, 2008 WL 10632524, at *7.

[62] *Id.* at *9–11.

turned to the question of whether the PAA could violate the rights of nontargeted U.S. persons through incidental collection.[63] The FISCR found the concern over incidental collection "overblown."[64] The government, the FISCR wrote, assured the court that "it does not maintain a database of incidentally collected information from nontargeted U.S. persons, and there is no evidence to the contrary."[65] Following a largely redacted portion of the opinion, the court rejected one argument of the petitioner as premature, since "petitioner has not yet experienced the type of harm about which it complains."[66] The "bare possibility" of the redacted unlawful acquisition was not enough for the court to grant relief.[67] The court therefore upheld the PAA.

In re Directives "ma[de] new law" when it recognized the foreign intelligence surveillance exception to the Fourth Amendment's warrant requirement.[68] But although it ruled against the company on the merits, it also, as Rozenshtein notes, was an early case that found a technology company had standing to assert its users' rights.[69]

(b) Clapper v. Amnesty International USA. — In *Clapper*, the plaintiffs were "attorneys and human rights, labor, legal, and media organizations" who believed that their sources, clients, or colleagues were likely targets of section 702 surveillance.[70] Because of the threat of government surveillance, the plaintiffs claimed, they had to take costly measures to maintain their privacy — including adopting technological evasion measures, traveling abroad to have the conversations in person, or just ending certain kinds of communications altogether.[71] In an opinion by Justice Alito,[72] the Supreme Court held that this harm was too speculative to constitute an injury in fact for the purposes of the standing doctrine.[73] An injury must be imminent to be cognizable, Justice Alito said, and that meant it had to be "certainly impending."[74]

---

63 *Id.* at *11.

64 *Id.*

65 *Id.*

66 *Id.* at *12.

67 *Id.*

68 Steve Vladeck, *More on* Clapper *and the Foreign Intelligence Surveillance Exception*, LAWFARE (May 23, 2012, 3:32 PM), https://www.lawfareblog.com/more-clapper-and-foreign-intelligence-surveillance-exception [https://perma.cc/44VC-5M9F].

69 *See* Rozenshtein, *supra* note 44, at 132.

70 568 U.S. 398, 406 (2013).

71 *Id.* at 406–07.

72 Justice Alito was joined by Chief Justice Roberts and Justices Scalia, Kennedy, and Thomas.

73 *Clapper*, 568 U.S. at 410. The district court had dismissed the case on summary judgment, finding that the plaintiffs had no standing to challenge section 702. Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 635 (S.D.N.Y. 2009). The Second Circuit, however, reversed, finding the plaintiffs had standing to challenge the law based on their objectively reasonable fear of being monitored and the costly steps they had taken to prevent surveillance. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 150 (2d Cir. 2011).

74 *Clapper*, 568 U.S. at 410 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

The plaintiffs could not establish standing to challenge the law because their theory of standing "relie[d] on a highly attenuated chain of possibilities" which did not "satisfy the requirement that threatened injury must be certainly impending."[75] For one, the plaintiffs couldn't prove the government had or would ever target someone with whom the plaintiffs regularly communicated.[76] At most, they could show that section 702 authorized that surveillance, but not that it "*mandate*[*d*] or *direct*[*ed*] it."[77] Another problem was that multiple laws authorized the government to target the foreigners located abroad whom plaintiffs were communicating with: even if the plaintiffs could show that those communications were intercepted, they could "only speculate" as to which law the government would use when doing so.[78] Justice Alito noted that the plaintiffs' theory of standing required the Court to assume that the FISA court would allow the government to target plaintiffs' foreign contacts.[79] The Court has been "reluctan[t] to endorse standing theories that rest on speculation about the decisions of independent actors."[80]

The Court also declined to find standing based on the measures plaintiffs had taken to avoid detection: costs did not change the fact that "the harm that they s[ought] to avoid [wa]s not certainly impending."[81] To hold otherwise, Justice Alito said, would allow plaintiffs to meet the "actual or imminent" burden with a showing of a subjective fear that is not entirely far-fetched for the mere "price of a plane ticket."[82] Plaintiffs also "had a similar incentive to engage in . . . countermeasures" before section 702 was enacted, leading the Court to conclude that their costs were "simply the product of their fear of surveillance" in general.[83] The Court also rejected the plaintiffs' reliance on cases that found a "chilling effect" on a regulated party to be a sufficiently cognizable injury; the plaintiffs mischaracterized the cases, it said, and they also could not assert a "chilling effect" when the chill was subjective and not substantiated by concrete facts about the government's actions.[84]

---

[75] *Id.*

[76] *Id.* at 411.

[77] *Id.* at 412.

[78] *Id.*; *see also id.* at 412–13.

[79] *Id.* at 413.

[80] *Id.* at 414; *id.* at 413–14 (citing Whitmore v. Arkansas, 495 U.S. 149, 159–60 (1990) (declining to find that the possibility that petitioner would get federal habeas relief but be convicted again upon state court retrial was an injury)).

[81] *Id.* at 416.

[82] *Id.* (quoting Amnesty Int'l USA v. Clapper, 667 F.3d 163, 180 (2d Cir. 2011) (Raggi, J., dissenting from denial of rehearing en banc)).

[83] *Id.* at 417.

[84] *See id.* at 419–20. For instance, in one of the *Clapper* plaintiffs' cited cases, *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167 (2000), the plaintiffs' injury was their inability to use a polluted river. *Id.* at 181–83. There was no dispute over whether the defendant's action caused the pollution: only over whether it was reasonable for the plaintiffs to avoid using the

Finally, the Court rejected the plaintiffs' argument that declining to find standing in a case like *Clapper* would leave section 702, and laws like it, effectively unchallengeable.[85] Justice Alito explained that even if that were true, that wouldn't be a reason to find standing.[86] And section 702 was also reviewable in other ways through processes specified in the statute.[87] But even outside those mechanisms, other parties still had standing to challenge the statute: citing *In re Directives*, Justice Alito noted that "electronic communications service provider[s] that the Government directs to assist in [section 702] surveillance may challenge the lawfulness of that directive before the FISC."[88] Thus, the Court held, the plaintiffs had no standing to challenge the suit.

Justice Breyer dissented.[89] He found that there was a "very high likelihood" that the government, acting under section 702, would "intercept at least some of [plaintiffs'] communications."[90] "[T]hat degree of certainty," he said, was sufficient for standing purposes.[91] The Constitution requires only a standard of "reasonable" or "high probability" of an actual injury: Justice Breyer would have applied that standard to find that the plaintiffs had standing.[92]

B. Technology Companies as Imperfect Surveillance Intermediaries

These two decisions have set up a dichotomy. In *Clapper*, the Court refused to allow members of civil society whose communications were likely to be intercepted by government surveillance to challenge the law, because the harm (interception) was too speculative without specific facts showing that the government (1) actually intercepted their communications, and (2) did so under the surveillance law being challenged. At the same time, the court in *In re Directives* found that a technology company had standing to assert those very same users' rights in challenging a surveillance law. The Supreme Court's decision in *Clapper* reaffirmed that holding in dicta.[93] In fact, it seemingly relied on technology companies' ability to challenge the law as an effective substitute

---

river. *Id.* at 183–84. Since the dispute in *Clapper* was over whether the government had "polluted the river," or used surveillance in the first place, rather than the reasonableness of the plaintiffs' chosen remedy, the *Clapper* Court said, the comparison was inapposite. *Clapper*, 568 U.S. at 419.

85 *Clapper*, 568 U.S. at 420.

86 *Id.* (quoting Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 489 (1982)).

87 *Id.* at 421.

88 *Id.* at 422.

89 Justice Breyer was joined by Justices Ginsburg, Sotomayor, and Kagan.

90 *Clapper*, 568 U.S. at 427 (Breyer, J., dissenting).

91 *Id.* at 431.

92 *Id.* at 441.

93 *See id.* at 422 (majority opinion).

for direct challenge by consumers when it said that declining to find standing in *Clapper* did not leave the law effectively unchallengeable.[94]

That is important. The two other avenues offered by the Court as alternative paths to judicial review will, in many cases, be inadequate to ensure real judicial oversight over the constitutionality of surveillance law. The first one, FISCR review, while more robust now than it has been, is deeply flawed. The USA FREEDOM Act of 2015[95] (Freedom Act) created an "amicus curiae," or a court-appointed advocate to make arguments to the FISC when it considers novel questions of law.[96] But aside from the amici, proceedings in front of the FISC remain ex parte; the amicus's role is limited to the questions certified to it by the FISC or FISCR, and they are not required to give input on questions of whether FISCR review is necessary.[97] And while the FISC's certification processes are not exactly "rubber stamping" applications, few applications are denied or even modified.[98] The second avenue — the government's notice obligations in criminal prosecutions — also leaves much to be desired. To begin, the government has not always complied with its notice obligations.[99] Though the Solicitor General in *Clapper* cited the government's disclosure obligations in criminal prosecutions as a potential avenue for standing, the government, at the time, had "*never given . . . notice to any criminal defendant*" even though the law had been operating for six years.[100] Some also worry that the nature of foreign intelligence information leaves the door open to parallel construction, or reconstructing FISA-obtained information through conventional

---

[94] *Id.* at 420–22.

[95] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act (USA FREEDOM Act) of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in scattered sections of 18 and 50 U.S.C.).

[96] *Id.* § 401 (codified at 50 U.S.C. § 1803).

[97] Chad Squitieri, *The Limits of the Freedom Act's Amicus Curiae*, 11 WASH. J.L. TECH. & ARTS 197, 204–09 (2015).

[98] Erika Eichelberger, *FISA Court Has Rejected .03 Percent of All Government Surveillance Requests*, MOTHER JONES (June 10, 2013, 5:30 PM), https://www.motherjones.com/crime-justice/2013/06/fisa-court-nsa-spying-opinion-reject-request/ [https://perma.cc/R9FJ-G8JD]; *see also* Marcy Wheeler, *Confirmed: The FISA Court Is Less of a Rubber Stamp Than Article III Courts*, EMPTYWHEEL (June 28, 2017), https://www.emptywheel.net/2017/06/28/confirmed-the-fisa-court-is-less-of-a-rubber-stamp-than-title-iii-courts/ [https://perma.cc/R946-8LJP] (providing figures). *But see* Conor Clarke, Essay, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125, 126 (2014) (arguing win/loss ratios are poor measures of FISC's efficacy).

[99] *See* Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, JUST SECURITY (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again [https://perma.cc/5V2M-4CW9].

[100] SAVAGE, *supra* note 33, at 559; *see also* Andrew Crocker, *EFF and ACLU Ask Appeals Court to Find Section 702 Surveillance Unconstitutional*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Oct. 24, 2017), https://www.eff.org/deeplinks/2017/10/eff-and-aclu-ask-appeals-court-find-section-702-surveillance-unconstitutional [https://perma.cc/PST9-NZWV] (noting that the government informed defendants only after the Snowden revelations).

investigative tools, thus allowing the government to avoid having to give notice of its use of FISA-obtained information (and preventing that defendant from having standing to challenge its constitutionality).[101]

That leaves the third avenue offered by Justice Alito: challenges by technology companies. If technology companies are the only actors who have standing to challenge some surveillance laws, the question must be asked: should they be? That is, can technology companies be trusted to zealously advocate for consumers' Fourth Amendment rights, and are they the actors best suited to shoulder that responsibility?

1. Technology Companies' Incentives. — Rozenshtein argues that technology companies "have powerful incentives to resist government surveillance" in the wake of the Snowden revelations.[102] He lays out two types of incentives. The first is cost: aside from lowering companies' costs of compliance with government surveillance, "resistance [is] an opportunity for product differentiation."[103] A foreign company competing with American service providers might "lobby for old-fashioned protectionism" in its home country by presenting American companies as tools of the U.S. surveillance state, and resisting surveillance at home is one way to counter that perception.[104] U.S. companies might also be financially required to resist surveillance because of foreign regulators. Indeed, as Rozenshtein writes, these incentives are "not merely theoretical": the European Court of Justice's (ECJ) decision in *Schrems v. Data Protection Commissioner*,[105] invalidating a European-American agreement on cross-border data flows based on privacy concerns, threatened to cost American companies billions.[106]

The second set of incentives put forth by Rozenshtein is ideological. Many in Silicon Valley, Rozenshtein argues, subscribe to the "Californian Ideology," or a "countercultural," "laissez-faire," and "libertarian" approach to life and work that is fundamentally incompatible with the surveillance state.[107] Though individual engineers and managers might

---

101 *E.g.*, John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 5:19 AM), https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805 [https://perma.cc/L88N-7E4S].

102 Rozenshtein, *supra* note 44, at 115.

103 *Id.* at 116 (citing Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J., 293, 340 (2011)).

104 *Id.* at 117.

105 Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362 [https://perma.cc/EU5D-UDSP].

106 Rozenshtein, *supra* note 44, at 118 (citing Richard Barbrook & Andy Cameron, *The Californian Ideology*, 6 SCI. AS CULTURE 44 (1996)).

107 *Id.*

not have the Californian ideology, managers still have the incentive to maintain the façade for "recruiting and morale purposes."[108]

Rozenshtein does acknowledge that Silicon Valley's incentives to resist surveillance are not unshakable. Companies in the past have been complicit with extensive government surveillance, shown willingness to trade in user data, and enabled government surveillance through creating the infrastructure.[109] Rozenshtein acknowledges the possibility that resistance to surveillance is a "pendulum [that] may well swing back," but he argues that companies present resistance to government surveillance that makes them worth studying as intermediaries.[110]

That might be true, but it doesn't answer the normative questions: When the avenues of challenging surveillance directly are so limited for members of American civil society, is the fact that technology companies are able to challenge surveillance enough? Will the incentives that brought Yahoo to challenge the directives it received under the PAA hold, or will the "pendulum swing back" and leave companies with the ability but without the will to challenge surveillance laws? It well may. While technology companies have financial incentives to challenge surveillance, they also have powerful financial incentives not to. They are rational actors: when it is worth their while to resist surveillance, they will. But especially in the standing arena, it is easy to see instances in which it will *not* be worth their while.

(a) Technology Companies as Rational Actors. — Whatever ideological or financial incentives they may have to resist surveillance, technology companies are, above all, just that — companies, with a fiduciary duty to their shareholders to maximize profit. When that profit motive conflicts with other ideals, it will, more often than not, win. Examples of technology companies acting contrary to their stated ideals, or the so-called Californian ideology, are countless. One might wonder whether Google broke its famous vow not to be evil when it lobbied for the Registrar of Copyrights to be fired because she was too protective of artists' and creators' rights[111] — certainly, the countercultural Californian ideology might have something to say about that. Even companies who market themselves based on their protections of user privacy aren't immune to making different decisions when push comes to pecuniary shove. From early on, WhatsApp made a name for itself as a privacy champion: Its founder promised in 2009 that "[w]e have not, we do not, and we will not ever sell your personal information to anyone. Period.

---

[108] *Id.* at 119.

[109] *Id.* at 120–21.

[110] *Id.* at 121.

[111] David Pridham, *How Google Tries to Buy Government*, FORBES (July 19, 2017, 1:57 PM), https://www.forbes.com/sites/davidpridham/2017/07/19/how-google-tries-to-buy-government/ [https://perma.cc/2SAV-ZNUQ].

End of story."[112] But the story didn't quite end there; in 2014, Facebook bought WhatsApp, and two years later WhatsApp changed its privacy policy to allow data sharing between it and Facebook for the first time.[113] And when companies do choose to fight for privacy protections, it is often *because*, not in spite, of their profit motives. Apple's decision to go to bat for end-to-end encryption might have won it friends in the privacy and civil liberties advocacy community, but it was also a savvy business move.[114] As Rozenshtein notes, Apple, compared to its competitors, relies far less on third-party access to user data; its defense of user privacy could just as credibly be seen as an "assault on the principal revenue scheme of its competitors."[115] Indeed, some companies' business models depend on access to user data: think Google's ad business.

Above all, "technology companies want to create and sell products and services in order to make as much profit as possible and increase market share, and eventually attain market dominance in core and new markets."[116] Sometimes, those activities will be better served by complying with the law; at other times, those activities will require some resistance and effort to change existing law. "Pre-Snowden, these companies arguably benefited from a closer degree of complicity with the U.S. government, which promoted their products and services as tools to further U.S. foreign policy democracy."[117] But after the Snowden revelations, companies had to convince their customers both domestically and abroad "of their independence from the U.S. government" — because it was financially beneficial for them to do so.[118]

That doesn't mean that technology companies haven't, on the whole, done more to protect privacy in the post-Snowden landscape than they have to hinder it. That is only to say that they might not always do so. It is to say that technology companies are large, complex entities that are subject to government regulation and that have contractual relationships with the federal government, and that might therefore make decisions on whether to align with government interests with their regulatory interests and contractual relationships in mind.[119] Indeed, most

---

[112] Brian Barrett, *WhatsApp's Privacy Cred Just Took a Big Hit*, WIRED (Aug. 25, 2016, 12:16 PM), https://www.wired.com/2016/08/whatsapp-privacy-facebook/ [https://perma.cc/DL5D-L6WT].

[113] *Id.*

[114] *See* Rozenshtein, *supra* note 44, at 138.

[115] TIM WU, THE ATTENTION MERCHANTS 336 (2016), *quoted in* Rozenshtein, *supra* note 44, at 138.

[116] Stephanie Hare, *For Your Eyes Only: U.S. Technology Companies, Sovereign States, and the Battle over Data Protection*, 59 BUS. HORIZONS 549, 551 (2016).

[117] *Id.*

[118] *Id.*

[119] *Cf.* ROBERT AXELROD, THE EVOLUTION OF COOPERATION 113–17 (1984) (describing how in an iterated prisoner's dilemma game — or one played by the same players over a period of time with scores aggregated across games — the most successful players are those who do not defect first but instead cooperate).

American technology giants do not interface with the government only over surveillance battles. Rather, these companies are repeat players. They spend millions lobbying the government on a whole range of issues — for instance, one analysis found that major tech players lobby the government on as many as a hundred issues a year.[120] To take a snapshot in time, at least one observer noted that technology companies were "largely absent" from the debate over section 702 renewal taking place in Washington in mid-2017.[121] But Washington in late 2017 was also debating possible tax reforms — tax reforms from which technology giants stand to see massive gains.[122] It is impossible to say whether Silicon Valley's silence over section 702 reform can be attributed directly to its interests in currying favor with lawmakers who were reforming the tax code. But it is enough, perhaps, to note that we would not be asking this question of individual consumers, who are not repeat players and therefore do not have longstanding and unrelated regulatory interests they must consider in challenging surveillance policies or bringing a lawsuit. Sometimes, then, it will be more financially beneficial for companies to challenge government surveillance. Sometimes it will not. And when the doors to the federal courts are open only to the technology companies, "usually but not always" isn't good enough.

This is especially true because technology companies' incentives to assert standing in the kind of challenge brought in *Clapper* aren't always the same as they are to challenge other forms of surveillance overreach. For instance, some commentators point to the scale of loss companies suffered when the ECJ invalidated the U.S.-E.U. Safe Harbor framework for data sharing, and the companies' resulting advocacy for Privacy Shield, as an example of financial incentives causing technology companies to advocate for increased privacy protections.[123] But the ECJ's decision wasn't motivated by concern for Americans' rights — it was motivated by concern for Europeans, whom the American government can constitutionally spy on.[124] There is no ECJ to put its thumb on the scale for Americans at home — and since an American technology com-

---

[120] Brian Fung & Hamza Shaban, *Want to Understand How Dominant Tech Companies Have Become? Look at the Number of Issues They Lobby On.*, WASH. POST (Aug. 31, 2017), http://wapo.st/2gtcimt [https://perma.cc/YA3K-MPU6].

[121] Dustin Volz, *Silicon Valley Mostly Quiet in Internet Surveillance Debate in Congress*, REUTERS (July 18, 2017, 4:27 PM), https://www.reuters.com/article/us-usa-intelligence/silicon-valley-mostly-quiet-in-internet-surveillance-debate-in-congress-idUSKBN1A32B3 [https://perma.cc/C5U8-XQRT].

[122] Shawn Tully, *How Tax Reform Could Make Apple a $1 Trillion Company*, FORTUNE (Oct. 17, 2017), http://fortune.com/2017/10/17/apple-tax-reform-trillion/ [https://perma.cc/79P5-JD37].

[123] *See supra* note 106 and accompanying text; *see also* Volz, *supra* note 121.

[124] Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 ¶¶ 30–33 (Oct. 6, 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362 [https://perma.cc/EU5D-UDSP].

pany is likely to lose a challenge trying to vindicate the Fourth Amendment rights of foreigners located abroad (as Yahoo lost in *In re Directives*), it might not have the same incentive to bring a challenge to vindicate Americans' rights as it would to appease European regulators.

As for the view that American consumers will drive technology companies to stand up to improper government surveillance, the fact is that the scale of market penetration by major technology companies makes it difficult for the market to punish companies for not adequately resisting government surveillance. Sixty-nine percent of American internet users are active on Facebook.[125] While users may say they care about privacy, they're ultimately more likely to prize convenience in their choice of online platforms.[126] What seems more likely to happen is market fractionalization: a minority of users who prioritize privacy move to privacy-friendly platforms like Signal, with those that don't staying on the major platforms. Economic incentives, therefore, seem insufficient to ensure that companies zealously advocate for users' rights.

(b) The Shield of Secrecy. — The secrecy with which intelligence work is conducted impacts the extent to which companies have financial incentives to advocate for more privacy, insulating them from market consequences for compliance. Proceedings before the FISC are classified and largely ex parte, meaning that the work of constructing and interpreting surveillance law takes place largely out of the public eye and without public input.[127] The Freedom Act reformed some of that through requiring the FISC to declassify significant opinions.[128] However, the government has been reluctant to retroactively declassify pre–Freedom Act opinions,[129] and the law leaves the FISC with discretion

---

125 *How Does Twitter and Facebook's Penetration Compare in Different Markets?*, FORBES: GREAT SPECULATIONS (Jan. 8, 2016, 1:43 PM), https://www.forbes.com/sites/greatspeculations/2016/01/08/how-does-twitter-and-facebooks-penetration-compare-in-different-markets/ [https://perma.cc/CXE5-WE3Q].

126 *See, e.g.*, Cory Doctorow, *Why Is It So Hard to Convince People to Care About Privacy?*, THE GUARDIAN (Oct. 2, 2015, 6:36 AM), https://www.theguardian.com/technology/2015/oct/02/why-is-it-so-hard-to-convince-people-to-care-about-privacy [https://perma.cc/HY2X-83VJ]; Hayley Tsukayama, *People Care More About Convenience than Privacy Online*, WASH. POST (Oct. 7, 2014), http://wapo.st/10Kohib [https://perma.cc/Y9UR-8YVP]; *see also* DANIELLE KEHL ET AL., NEW AM.'S OPEN TECH. INST., SURVEILLANCE COSTS 11 (2014), https://s3.amazonaws.com/www.newamerica.org/downloads/Surveilance_Costs_Final.pdf [https://perma.cc/2W3P-2T8Z] (arguing that users who prefer a more privacy-oriented platform might not use one because of the cost of switching or lack of alternative platforms).

127 Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), https://nyti.ms/2mCBjNt [https://perma.cc/FV4F-MVQN].

128 USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 402(a)(2), 129 Stat. 268, 281–82 (codified at 50 U.S.C. § 1872 (Supp. III 2016)).

129 Aaron Mackey, *USA FREEDOM Act Requires Government to Declassify Any Order to Yahoo*, DEEPLINKS BLOG (Oct. 7, 2016), https://www.eff.org/deeplinks/2016/10/usa-freedom-act-requires-government-declassify-any-order-yahoo [https://perma.cc/R7UW-G8ZD].

on whether to declassify an entire opinion or only a redacted or summarized version of it.[130] That discretion is a shield. For instance, the FISC issued its first post–Freedom Act ruling allowing the NSA to collect telephone records on December 31, 2015. The order, declassified in April 2016, was redacted of a key piece of information: the names of the telecommunications providers who were the target of it.[131]

Classified proceedings are only the beginning of the problem. Most surveillance orders to companies, including, for instance, National Security Letters (NSLs) — a kind of administrative subpoena under which the government can elicit very revealing records — are often accompanied by gag orders.[132] The constitutionality of collecting electronic communications transactional records (ECTRs), or the kind of revealing noncontent information that the government gets through NSLs, is outside the scope of this Chapter. For our purposes, the important fact is that there is a debate over their constitutionality, and they thus implicate the same problem as section 702 — the inability of users who don't know about surveillance to challenge its constitutionality. Though companies sometimes challenge these gag orders — as Facebook recently did[133] — the decision to challenge a gag order and reveal to the users that their communications are being monitored is at the company's own discretion. As such, the company has the option of insulating itself from the kind of financial incentive structure Rozenshtein describes, or from any public pressure. The Department of Justice (DOJ) recently settled a lawsuit by Microsoft about the constitutionality of gag orders.[134] As part of the settlement, DOJ agreed to adopt guidelines on the use of gag orders, vowing to end their routine use.[135] But the policy does not apply to FISC orders or NSLs, leaving the door open to continued abuse of the gag order process in the national security arena to insulate companies from disclosure.[136]

That secrecy is why companies, for decades, complied with surveillance orders with few consequences.[137] Of course, given the frequency

---

[130] Dakota S. Rudesill, *It's Time to Come to Terms with Secret Law: Part I*, JUST SECURITY (July 20, 2016), https://www.justsecurity.org/32120/time-terms-secret-law-part/ [https://perma.cc/ELJ7-257H].

[131] Mark Hosenball, *Secret U.S. Court Issues First Order for Phone Data Under New Law*, REUTERS (Apr. 19, 2016, 5:55 PM), http://www.reuters.com/article/us-usa-surveillance-court/secret-u-s-court-issues-first-order-for-phone-data-under-new-law-idUSKCN0XG2UR [https://perma.cc/H234-URF8].

[132] Jonathan Manes, *Online Service Providers and Surveillance Law Transparency*, 125 YALE L.J.F. 343, 349–51 (2016).

[133] *See infra* pp. 1760–61.

[134] Ellen Nakashima, *Justice Department Moves to End Routine Gag Orders on Tech Firms*, WASH. POST (Oct. 24, 2017), http://wapo.st/2yNETdt [https://perma.cc/LEK9-K6BM].

[135] *Id.*

[136] *Id.*

[137] *See supra* ch. 1, p. 1725.

of surveillance leaks, companies run the risk that their acquiescence with surveillance will be leaked — as Rozenshtein points out, a key legacy of the Snowden disclosures is breaking the veil of secrecy behind technology company compliance with secret surveillance orders.[138] But not every instance of compliance will leak, if only because of the law of large numbers. In the last six months of 2016, Google received between 0 and 499 NSLs implicating between 1000 and 1499 users or accounts.[139] In the same reporting period, Google received between 500 and 999 FISA requests for content implicating between 35,000 and 35,499 users or accounts.[140] The sheer number of requests makes accountability through public shaming and leaks impractical on a macro scale. And indeed, as discussed above, it is doubtful there is much consumer elasticity even in response to major leaks (due to technology giants' market penetration).[141] Secrecy thus serves, at least partially, to insulate companies from the consequences of complying with the surveillance state.

C. Benefits of Users as Their Own Advocates

Whatever incentives technology companies might have to protect users' rights, no one is more suited to assert the violation of a right than the person whose right has been violated. Facebook itself admitted this in a recent case. In *Facebook v. United States*,[142] Facebook challenged a nondisclosure order that prevented it from telling users that the government was seeking access to their private Facebook accounts.[143] Facebook fought the order, leading the D.C. Court of Appeals to allow it to solicit public input from civil society advocates.[144] Notably, Facebook did not contest the underlying constitutionality of the warrants,[145] although it would have had standing to do so under *In re Directives*. Rather, it sought to "vacate the NDO so that it could provide its users with

---

138 Rozenshtein, *supra* note 44, at 115–16.

139 *United States National Security Requests*, GOOGLE: TRANSPARENCY REP., https://transparencyreport.google.com/user-data/us-national-security [https://perma.cc/8X8C-C4GL].

140 *Id.*

141 *See supra* p. 1758.

142 The records of this case are sealed. *See* Notice to Potential Amici Curiae at 1, Facebook, Inc. v. United States, Nos. 17-SS-388, 17-SS-389, 17-SS-390 (D.C. 2017), https://www.aclu.org/legal-document/facebook-v-united-states-notice-potential-amici-curiae [https://perma.cc/SF7P-RHZX].

143 *Id.* at 1–2.

144 *Id.*; *see* Phillip Takhar, Facebook v. United States*: Facebook Cites First Amendment in Challenge to Government Non-disclosure Order*, JOLT DIG. (July 30, 2017), http://jolt.law.harvard.edu/digest/facebook-v-united-states-facebook-cites-first-amendment [https://perma.cc/N5K6-CZ28].

145 Brief of Amici Curiae the American Civil Liberties Union et al. in Support of Appellant and Reversal at 6, Facebook Inc. v. United States, Nos. 17-SS-388, 17-SS-389, 17-SS-390 (D.C. 2017) [hereinafter Brief of Amici Curiae], https://www.aclu.org/legal-document/facebook-v-united-states-amicus-brief [https://perma.cc/8BMQ-ZW47].

notice of the Warrants and an opportunity to object to them before Facebook produced responsive records to the government."[146] In its amicus brief, the ACLU argued that here, "[a]s in many cases, the users are the people best positioned to show why execution of the warrants would infringe their constitutional rights before the fact of production has effectuated the very harms the First and Fourth Amendments are meant to prevent."[147] But they cannot do so without notice.

Nor should companies necessarily have to shoulder the burden. In its brief in *Facebook*, the ACLU observed that "[i]t would be unreasonable to expect Facebook, with more than 150 million users in the United States, and other companies, most of which have far fewer resources, to challenge every overbroad warrant served for user information."[148] That is true. Companies are not civil liberties organizations. They do not exist to advance their users' civil rights. When users' rights happen to intersect with a company's financial interests, the company should certainly assert those rights for the mutual benefit of the company and users. But when they don't, there is no reason to think a technology company can and should be responsible for its users' rights.

1. A World Without Intermediaries. — There is no guarantee that a user asserting a constitutional claim would find a more favorable outcome than a company asserting that user's claim under the same set of facts. Some suspect that standing decisions "in close cases may be guided more by the courts' instincts toward the merits than by an independent determination of the parties' eligibility to invoke jurisdiction."[149] Thus, it might be argued that it is irrelevant who brings the challenge once it is brought: the outcome will be the same regardless. But even if the outcome would be the same on the merits, or even if a technology company would be more likely to succeed,[150] there may be cases where only an individual *could* bring the suit in the first place.

It is a point worth making that it is, essentially, a coincidence of technology that companies can even serve as intermediaries in this

---

146 Notice to Potential Amici Curiae, *supra* note 142, at 2.

147 Brief of Amici Curiae, *supra* note 145, at 6.

148 *Id.* at 6 n.3.

149 Mark C. Rahdert, *Forks Taken and Roads Not Taken: Standing to Challenge Faith-Based Spending*, 32 CARDOZO L. REV. 1009, 1016 (2011). *But see* Richard H. Fallon, Jr., *The Fragmentation of Standing*, 93 TEX. L. REV. 1061, 1069 (2015).

150 For instance, as Professor Daphna Renan points out, the Fourth Amendment's system of rules is transactional in nature: that is, it contemplates an encounter between one police officer and one citizen. Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1051 (2016). This framework is poorly suited to assessing the constitutionality of the kind of programmatic, dragnet collection that characterizes modern surveillance. *Id.* at 1056. Thus, for example, a technology company could potentially have more success showing the aggregate effects of mass surveillance and arguing that the activity is unconstitutional in the aggregate even if individual instances of the surveillance might not be, *see id.* at 1056–60, as it would have access to a larger dataset and the ability to search it for patterns. But as discussed in section B, it is doubtful that it would have the same incentives to do so as would users with access to the same dataset.

space. That is, the only reason that companies have standing to challenge the law is that the government is technologically incapable of collecting the foreign intelligence information it seeks without issuing directives to companies. Consider this hypothetical: Pursuant to a law passed by Congress, the government selects a U.S. person at random once a week and collects her information, using technology that is not reliant on any company's cooperation, without probable cause. This person never finds out. Is this a clearly unconstitutional action? Yes. But who can challenge it? Like in *Clapper*, we would know to a virtual certainty that there is a class of people who are being harmed as a result of a constitutionally questionable government action. But also like in *Clapper*, we have no way of knowing who these people are. Even people who, based on press leaks or the hypothetical lottery's targeting practices, believe that they are being targeted by the program could not prove a "threatened injury" that is "certainly impending" — like the *Clapper* plaintiffs, they would have no actual knowledge of any specific facts in support of their constitutional claim of harm.[151]

As the *Clapper* Court noted, doctrinally, the fact that if "respondents have no standing to sue, no one would have standing to sue, is not a reason to find standing."[152] But as a matter of *policy*, it should perhaps trouble us that one of the few mechanisms for judicial review of programmatic government surveillance turns on the technological exigencies of a particular mode of surveillance in a world of rapidly evolving technology.[153] The world in which intermediaries are not necessary for government surveillance may be far off; given the omnipresence of technology in facilitating our communications, it might never exist. But it may just as easily be closer than we think. Indeed, there's some evidence that the government is already developing surveillance capabilities that allow it to intercept communications without the aid of service providers, though the process is expensive and time-consuming.[154] If the government develops that capability and deploys it in a way that infringes on U.S. persons' constitutional rights, our system is not equipped to ensure this practice is reviewed for its constitutionality in an adversarial court.

---

151 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).

152 *Id.* at 420 (quoting Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 489 (1982)).

153 *Cf.* Richard M. Re, *Relative Standing*, 102 GEO L.J. 1191, 1196–97 (2014) (arguing that the plaintiff with "the greatest stake in obtaining a specific remedy for a particular violation" should have standing, *id.* at 1196, and that relative standing "already drives the result in a wide range of modern standing cases," *id.* at 1197).

154 Kim Zetter, *NSA Laughs at PCs, Prefers Hacking Routers and Switches*, WIRED (Sept. 4, 2013, 6:30 AM), https://www.wired.com/2013/09/nsa-router-hacking/ [https://perma.cc/RJ4P-ZZ2N].

D. Opening the Courts to Individuals

If technology companies cannot always be trusted (or might not always be able) to bring suits on behalf of consumers, then what is required to make sure that the constitutionality of surveillance laws has its day in court? One answer may be "more information." The problem in *Clapper* was, in a sense, evidentiary: someone, somewhere might be experiencing the kind of harm that would have led the Court to find an injury in fact, but the plaintiffs could not prove that this someone was in fact them. More rigorous disclosure requirements might make it easier for plaintiffs to bridge that evidentiary gap, thus allowing them to bring their own challenges. This solution will, understandably, likely prove quite unpopular with the intelligence community — while the government undoubtedly keeps many more secrets than it needs to,[155] a lot of surveillance is highly classified for a good reason, and it would likely be too tall an order to ask for individual surveillance decisions (of the kind that would be needed to confer standing on any one plaintiff) to be more regularly disclosed.[156] A middle ground may be found in procedural rights cases. In a number of contexts, Congress has essentially relaxed the normal Article III requirement of an injury in fact by creating a procedural right that may be vindicated in court.[157] One might imagine a statute granting a right to constitutional review of surveillance decisions, or a right to know whether one was unconstitutionally surveilled, that could be asserted by anyone and vindicated in court.

Another, similar option would be to adopt a legal fiction used in other legal contexts to vindicate other kinds of unknowable harms. The standing problem in surveillance cases boils down to the information gap: who has standing to challenge a law when the person who is truly harmed by it does not know it, nor has the capacity to know it?[158] But courts have come up with an answer to that question in other contexts. Think of what happens when the rights of children end up in court. An infant does not have the ability to truly know whether she is being harmed. But in that situation, courts often appoint a "guardian ad litem" to argue for the best interests of the child. The idea that there is a meeting of the minds between the child and the attorney is, at best, a

---

155 Abbe David Lowell, Opinion, *The Broken System of Classifying Government Documents*, N.Y. TIMES (Feb. 29, 2016), https://nyti.ms/2C12fyp [https://perma.cc/ZKW8-5NVZ].

156 *See* Shreve Ariail, *The High Stakes of Misunderstanding Section 702 Reforms*, LAWFARE (Dec. 6, 2017, 7:00 AM), https://www.lawfareblog.com/high-stakes-misunderstanding-section-702-reforms [https://perma.cc/2EJ3-U5N8] (describing section 702 as essential to national security and criticizing reform as misguided).

157 *See* Evan Tsen Lee & Josephine Mason Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 191, 199 (2012).

158 Scott Michelman, *Who Can Sue over Government Surveillance?*, 57 UCLA L. REV. 71, 80 (2009).

legal fiction: the advocate makes an argument for the best interests of the child not based on any of the child's stated desires but rather on the advocate's assessment of the law and the facts before him. A court could do the same in the surveillance context — that is, appoint an advocate for the person whose rights are being violated but who doesn't have access to the necessary information.[159] This, admittedly, doesn't solve the problem that section B identifies: there is still an information gap that could lead to a different outcome on the merits. But it still, at the very least, ensures that an advocate whose interests (unlike a technology company's) are always aligned with that of the harmed party is available to bring a facial challenge to the court's attention.[160]

A final possibility may involve the courts themselves. The Second Circuit below as well as the dissenters in *Clapper* both offered an alternate formulation of a standard for standing: whether there is a *reasonable probability* of harm.[161] The European Court of Human Rights (ECHR), for instance, has said that a plaintiff may establish victim status even if he has not shown that he was in fact impacted by the challenged law and even if domestic remedies are available if he is able to show that "due to his personal situation, he is potentially at risk of being subjected to" the challenged measure.[162] If the Supreme Court were to move away from the *Clapper* majority's approach and adopt a similar standard, individual plaintiffs would have a far easier time establishing standing in surveillance cases. Though this would require overruling or distinguishing *Clapper*, the Court showed willingness to do so in the opinion itself: in a footnote, Justice Alito noted that precedent does "not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about," but that the *Clapper* plaintiffs

---

159 This would more closely resemble the proposals for a FISC "special advocate" that Congress rejected when it created the more limited FISC amicus curiae. *See* Squitieri, *supra* note 97, at 200–01.

160 *See The Supreme Court, 2014 Term — Leading Cases*, 129 HARV. L. REV. 181, 241 (2015) (discussing facial challenges under the Fourth Amendment).

161 Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011) (stating the standard for standing as whether there was "an objectively reasonable likelihood that the plaintiffs' communications are being or will be monitored under" section 702); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 427–30, 441 (2013) (Breyer, J., dissenting) (finding that based on "(1) similarity of content, (2) strong motives, (3) prior behavior, and (4) capacity," there was "a very strong likelihood that the Government will intercept . . . plaintiffs' communications," *id.* at 430, and that this created a "reasonable" or "high probability" of injury, which was sufficient to satisfy his formulation of the constitutional standard, *id.* at 441).

162 Zakharov v. Russia, App. No. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, ¶ 171 (Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324 [https://perma.cc/AT9E-9ZA7]. The ECHR also allows plaintiffs to challenge laws facially without showing that they were even potentially surveilled if they can show that the law cannot be challenged domestically, thereby causing "widespread suspicion of abuse." *Id.* As discussed in *Clapper*, the Supreme Court has rejected this "effectively unchallengeable" approach. *See Clapper*, 568 U.S. at 420; *see also supra* p. 1751–52.

failed to meet even that "substantial risk" standard.[163] Were the Court willing, this footnote could be a pathway toward "soft[ening] the impact" of *Clapper*'s seemingly strict test.[164]

E. Conclusion

Let's return to our journalist and her source. The government has lawfully targeted communications to or from Viktor, a highly placed Russian intelligence official with knowledge on Russia's effort to hack the U.S. election — unbeknownst to Journalist Jada, who often communicates with Viktor. As section A of this Chapter explains, Jada can't challenge the collection under the Supreme Court's jurisprudence in *Clapper*. But her service provider, Google, might be able to do so under the FISCR's decision in *In re Directives*. Can Jada trust Google to challenge the government's actions on her behalf? Section B of this Chapter argues that she cannot. Because technology giants like Google are companies, and thus have incentives that are much different than Jada's own, they may choose not to challenge the surveillance state when it suits them. And as technology develops, service providers like Google, section C notes, may be dealt out of the equation altogether — leaving Jada with no recourse to challenge the government's actions. As section D argues, some reforms could remedy the situation. For instance, if the court were to adopt a probabilistic definition of "injury," as has the ECHR, Jada could bring a suit and assert her rights.

Technology companies are not angels, nor are they demons. They are just that — companies. Though an accident of technology and standing doctrine has put them in a place where they can vindicate rights not available to their users, they cannot, nor should they be expected to, act as faithful stewards of their users' rights in all places and at all times. The incentives are too misaligned, the burdens too great, and the risks of underenforcement too high for the courthouse's doors to be open exclusively to a company when its users are left outside. And that is precisely where the current jurisprudence of standing has left the courthouse doors: closed to users, who instead are dependent on technology companies to advocate for them in an age of ever-growing surveillance. Whatever shape reform takes, it ought to be cognizant of that.

---

[163] *Clapper*, 568 U.S. at 414 n.5.

[164] Amanda Mariam McDowell, Note, *The Impact of* Clapper v. Amnesty International USA *on the Doctrine of Fear-Based Standing*, 49 GA. L. REV. 247, 273–74 (2014).