CHAPTER ONE

COOPERATION OR RESISTANCE?: THE ROLE OF TECH COMPANIES IN GOVERNMENT SURVEILLANCE

Facebook received 32,716 requests for information from U.S. law enforcement between January 2017 and June 2017.[1] These requests covered 52,280 user accounts and included 19,393 search warrants and 7632 subpoenas.[2] In the same time period, Google received 16,823 requests regarding 33,709 accounts,[3] and Twitter received 2111 requests regarding 4594 accounts.[4] Each company produced at least some information for about eighty percent of requests.[5] In just six months, law enforcement agencies turned to technology companies to gather evidence for thousands of investigations. Of the many conclusions that one might draw from these numbers,[6] at least one thing is clear: technology companies have become major actors in the world of law enforcement and national security. In his recent article, Professor Alan Rozenshtein dubs these technology companies "surveillance intermediaries" — entities that sit between law enforcement agencies and the public's personal information, and that have the power to decide just how easy or difficult it will be for law enforcement to access that information.[7]

Surveillance intermediaries hold extraordinary power when they decide how to respond to government requests for information — power that may or may not be to the public's benefit. While intermediaries must comply with statutory and constitutional law governing law enforcement requests for information,[8] Rozenshtein explains that they still

---

[1] *Government Requests: United States, January 2017–June 2017*, FACEBOOK: TRANSPARENCY REP., https://transparency.facebook.com/country/United%20States/2017-H1/ [https://perma.cc/LMH4-XB5N].

[2] *Id.*

[3] *Requests for User Information*, GOOGLE: TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;time:Y2017H1;authority:US&lu=user_requests_report_period [https://perma.cc/LBZ8-L6H8].

[4] *United States of America*, TWITTER: TRANSPARENCY REP., https://transparency.twitter.com/en/countries/us.html [https://perma.cc/BCE5-GELY].

[5] *See* FACEBOOK, *supra* note 1 (85%); GOOGLE, *supra* note 3 (81%); TWITTER, *supra* note 4 (77%).

[6] *See, e.g.*, Alfred Ng, *Google Reports All-Time High of Government Data Requests*, CNET (Sept. 28, 2017, 5:11 PM), https://www.cnet.com/news/google-reports-all-time-high-of-government-data-requests/ [https://perma.cc/LN5Y-758E] (noting that the increased requests have led to privacy concerns).

[7] *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 105 (2018) ("By entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of *surveillance intermediaries*: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance.").

[8] Currently, surveillance intermediaries are subject to three major statutory constraints: the Wiretap Act of 1968, 18 U.S.C. § 2511 (2012), governing the interception of electronic and wire

hold a large degree of discretion when processing those requests: discretion in how critically they evaluate the legality of requests, in slowing down the process by insisting on proceduralism, and in minimizing their capacity to respond to legal requests by implementing encryption.[9] This discretion means that surveillance intermediaries determine, at least in part, the government's access to information about our personal relationships, professional engagements, travel patterns, financial circumstances, and much more. They also impact the government's ability to prevent terrorist attacks, solve murders, and locate missing children. In short, companies such as Facebook, Google, and Twitter are now responsible for decisions that have major consequences for our privacy, on the one hand, and our safety, on the other. This power is not the product of purposeful design — technology companies were not created in order to shield our information from, or deliver our information to, law enforcement agencies. Rather, the role of surveillance intermediary is one that technology companies happened to fall into by virtue of their omnipresence in our day-to-day lives.

As Congress and the judiciary are called upon to regulate technology companies under antitrust legislation,[10] they may also turn their attention to these companies' roles as surveillance intermediaries. It may not be ideal for private corporations to exercise so much power in determining the balance between privacy and security when it comes to government access to a wealth of information on individual people — but this is precisely the sort of determination that Congress and the judiciary are called upon to make all the time. In order to regulate the discretion of surveillance intermediaries, it is vital to understand the incentive structure driving intermediary behavior: How do surveillance intermediaries

---

communications; the Stored Communications Act of 1986, 18 U.S.C. §§ 2701–2712, governing access to stored information at rest; and the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.), governing the collection of foreign intelligence. The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.), amended the Wiretap Act and created the Stored Communications Act. In addition, the exchange of information between law enforcement and surveillance intermediaries must comply with the Fourth Amendment. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1025–31 (2010). While some statutory and constitutional requirements are clear and uncontroversial, others are subject to a variety of judicial interpretations. *See, e.g.*, Ann E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), http://wapo.st/1l9iiJZ [https://perma.cc/PG2W-5GVR] (describing federal magistrate judges' resistance to broad government requests for cell phone and other personal data).

[9] *See* Rozenshtein, *supra* note 7, at 122–25, 138–39.

[10] *See, e.g.*, Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 790–802 (2017); Joe Kennedy, *Should Antitrust Regulators Stop Companies from Collecting So Much Data?*, HARV. BUS. REV. (Apr. 17, 2017), https://hbr.org/2017/04/should-antitrust-regulators-stop-companies-from-collecting-so-much-data [https://perma.cc/SQ3X-DRGF]; Jonathan Taplin, Opinion, *Is It Time to Break Up Google?*, N.Y. TIMES (Apr. 22, 2017), https://nyti.ms/2p7Emhp [https://perma.cc/MM2U-U64V].

decide when to cooperate and when to resist? And how do these decisions vary between companies and over time? Understanding the answers to these questions is critical to predicting the behavior of large technology companies — in their role as surveillance intermediaries and beyond.

Much of the scholarship on surveillance intermediaries attempts to generalize their behavior, asking whether we can expect them to assist or resist government requests for information — in other words, do intermediaries mostly tend to cooperate with the government or obstruct the government? While there is surely value in this high-level analysis, this Chapter argues that such inquiries miss some of the finer nuances of the incentive structures driving intermediary behavior. The truth is, there are times when surveillance intermediaries cooperate with the government — perhaps too much — and there are times when surveillance intermediaries resist the government — perhaps too much — in response to situational incentives that may change over time and across companies. Regulators that seek to change the behavior of surveillance intermediaries to optimize for privacy and security must fully appreciate these incentives and the resulting diversity among intermediaries in order to develop an effective regulatory scheme.

Section A begins by highlighting two opposing views of surveillance intermediaries: that they serve to *assist* government surveillance by centralizing data storage, and that they serve to *resist* government surveillance by obstructing efforts to collect that data. Section A resolves this tension by presenting a more complicated portrait of surveillance intermediaries, a portrait that admits variation in responses to government surveillance requests over time, across companies, and in response to a variety of situational incentives. Section B considers several case studies of surveillance intermediary behavior in order to elucidate the complex web of incentives that generates the variation in their decisionmaking, as emphasized in section A. Finally, section C argues that there is reason to be hopeful: Certain institutional characteristics of a system in which large technology companies act as surveillance intermediaries provide significant advantages in both the privacy and national security realms. If regulators can find a way to align these companies' incentives with the public good, the resources and insights of intermediaries can be leveraged to improve both security and privacy.

A. Moving Away from Assistance vs. Resistance

Technology companies' approaches to their roles as surveillance intermediaries — and how easy or difficult they make it for the government to obtain data — vary significantly between companies and over time. Some commentators believe that this arrangement, on balance, leads to an inappropriate amount of cooperation between intermediaries

and law enforcement.[11] The centralization of communication through technology companies is thought to be a convenience for the government,[12] allowing it to "indulge its temptation to play Big Brother" by working with a small number of companies.[13] These companies can be persuaded to cooperate with law enforcement by appealing to their patriotism[14] and desire to maintain positive relationships with their regulators[15] — even in the absence of appropriate legal process.[16]

One example supporting this argument is AT&T's cooperation with the National Security Agency (NSA) in the years following 9/11. Leaked NSA documents from this time describe AT&T as an eager partner in surveillance beginning just "days" after such surveillance commenced in October 2001.[17] By striking a "partnership" with a single "highly collaborative" company, the NSA was able to gain access to an enormous amount of internet traffic.[18] According to the AT&T engineer who initially revealed the company's cooperation with the government, AT&T built an entire room in its headquarters that appeared to be solely dedicated to "copying the whole Internet" for the NSA.[19] AT&T did this despite the fact that the program was run without a clear legal basis from 2001 through 2008, at which point Congress passed a statute au-

---

[11] *See, e.g.*, TIM WU, THE MASTER SWITCH 249–52 (2010); Hannah Bloch-Wehba, *Process Without Procedure: National Security Letters and First Amendment Rights*, 49 SUFFOLK U. L. REV. 367, 379 (2016); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 904 (2008); Bruce Schneier, *The Trajectories of Government and Corporate Surveillance*, SCHNEIER ON SECURITY (Oct. 21, 2013, 6:05 AM), https://www.schneier.com/blog/archives/2013/10/the_trajectorie.html [https://perma.cc/DE6A-ZYH7].

[12] *Cf.* JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 117–18 (2008) (noting that traditional physical limitations do not exist in electronic surveillance).

[13] WU, *supra* note 11, at 252.

[14] *See* Rozenshtein, *supra* note 7, at 103–04.

[15] *See* Michaels, *supra* note 11, at 912–13. Indeed, at least one major telecommunications company claims that it faced retaliation in the form of cancelled government contracts after refusing to work with the National Security Agency (NSA) after 9/11 due to concern over "the legal implications of handing over customer information to the government without warrants." *Id.* at 912 (quoting Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006, 10:38 AM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm [https://perma.cc/2Q3Q-74UG]).

[16] *See id.* at 919 (discussing "the [h]andshake [i]ntelligence [p]artnership"); Bruce Schneier, *The Public-Private Surveillance Partnership*, SCHNEIER ON SECURITY (July 31, 2013), https://www.schneier.com/essays/archives/2013/07/the_public-private_s.html [https://perma.cc/FYR8-7DMZ].

[17] Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Aug. 15, 2015), https://nyti.ms/2jE59zh [https://perma.cc/M8VR-LKRM].

[18] *Id.*

[19] WU, *supra* note 11, at 249 (quoting Ellen Nakashima, *AT&T Gave Feds Access to All Web, Phone Traffic, Ex-Tech Says*, SEATTLE TIMES (Nov. 8, 2007), https://www.seattletimes.com/seattle-news/politics/att-gave-feds-access-to-all-web-phone-traffic-ex-tech-says/ [https://perma.cc/DLA9-AW7B]).

thorizing the program and granting full retroactive immunity for its participants.[20] It is clear that AT&T went above and beyond to facilitate government surveillance without much concern over the legality of that surveillance.

This story paints a bleak picture of AT&T undermining the legal structure built to protect its users' privacy rights. It shows that surveillance intermediaries are capable of providing the U.S. government with an enormous amount of data, far exceeding what they are legally required to turn over. It is an ominous incident in the history of intermediaries that should raise concerns about the incredible amount of power that a company like AT&T holds.

Other commentators, including Rozenshtein, have concluded that the rise of surveillance intermediaries is likely to impose constraints on government surveillance,[21] for better[22] or worse.[23] This is thought to be particularly true in the wake of the 2013 Snowden disclosures, which indicated that major technology companies were heavily involved in government surveillance.[24] The backlash to this revelation had a direct financial impact on U.S. companies, particularly due to the loss of foreign customers.[25] In order to save their reputations, technology companies have been publicly demonstrating their commitment to privacy and civil liberties over the past few years.[26] While there are surely ideological reasons[27] behind this shift, many commentators point to the strong profit incentives underlying this post-Snowden behavior.[28] A commitment to privacy is highly valued among customers at the moment and can serve as a valuable marketing tool.[29]

---

[20] Angwin, *supra* note 17. For more information about the reconsolidation of power under AT&T that led to this partnership, see WU, *supra* note 11, at 238–53.

[21] *See* Rozenshtein, *supra* note 7, at 116–17.

[22] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600 (2009) (noting that surveillance intermediaries could prevent government overreach despite permissive Fourth Amendment doctrine).

[23] *See* Rozenshtein, *supra* note 7, at 169–71.

[24] *Id.* at 115–16.

[25] *See* Janus Kopfstein, *Silicon Valley's Surveillance Cure-All: Transparency*, NEW YORKER (Oct. 1, 2013), https://www.newyorker.com/tech/elements/silicon-valleys-surveillance-cure-all-transparency [https://perma.cc/9QFQ-YPXV]; Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://nyti.ms/2nJdWCF [https://perma.cc/ST5Z-DDUZ] (citing predictions of post-Snowden losses ranging from $35 to $180 billion).

[26] *See, e.g.*, Brad Smith, *Protecting Customer Data from Government Snooping*, OFFICIAL MICROSOFT BLOG (Dec. 4, 2013), https://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/ [https://perma.cc/CY9M-L6T8].

[27] *See, e.g.*, Justin Lynch, *Suits and Hoodies: The Two Cybersecurity Cultures*, THE ATLANTIC (Feb. 27, 2015), https://www.theatlantic.com/technology/archive/2015/02/the-two-cybersecurity-cultures-suits-and-hoodies/386411/ [https://perma.cc/5AG6-BUNV].

[28] *See* Rozenshtein, *supra* note 7, at 116–18.

[29] *See id.*; CHARLIE SAVAGE, POWER WARS: INSIDE OBAMA'S POST-9/11 PRESIDENCY 570 (2015).

Evidence for this perspective can be found in the volume of litigation pursued by major technology companies challenging the government over requests for information in the years since the Snowden disclosures. Even putting aside the NSA and national security–related requests, surveillance intermediaries have been challenging law enforcement — including local law enforcement — on subpoenas and search warrants. In 2016, Microsoft quashed a search warrant from the Southern District of New York seeking data stored on servers in Ireland related to a narcotics case, arguing that the warrant violated the presumption against extraterritoriality.[30] That same year, Apple challenged the use of the All Writs Act[31] in the Eastern District of New York for a narcotics case,[32] and again, famously, in the Central District of California for a terrorism case.[33] In 2017, Facebook lost a challenge against the Manhattan District Attorney's Office for search warrants related to a disability fraud case.[34] Finally, in October 2017, the U.S. government, facing a lawsuit by Microsoft, developed strict guidelines on the use of gag orders by U.S. Attorneys.[35] These are just a few examples of major face-offs between surveillance intermediaries and the government, demonstrating the existence of a resistant band of technology companies fighting against perceived government overreach.

The rise of intermediary-initiated litigation paints a much more optimistic picture of surveillance intermediaries. It indicates that major technology companies are critically reviewing the legal orders they receive from the government and pushing back on government overreach when necessary. This resistance might make us foster confidence in our data stewards and the surveillance intermediary system.

Scholars who believe that surveillance intermediaries pave the way for lawless Big Brother–esque government surveillance are justified in their fears; as AT&T's post-9/11 behavior demonstrates, it is possible for

---

30 Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017).

31 28 U.S.C. § 1651 (2012).

32 *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

33 Apple Inc.'s Reply to Government's Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (C.D. Cal. Mar. 15, 2016), ECF No. 177.

34 James C. McKinley Jr., *Facebook Loses Appeal to Block Bulk Search Warrants*, N.Y. TIMES (Apr. 4, 2017), https://nyti.ms/2nUnybc [https://perma.cc/ES5Y-77VA].

35 Memorandum from Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Justice, to U.S. Attorneys et al. (Oct. 19, 2017), https://assets.documentcloud.org/documents/4116081/Policy-Regarding-Applications-for-Protective.pdf [https://perma.cc/26L2-7ENX]; Nick Wingfield, *U.S. to Limit Use of Secrecy Orders That Microsoft Challenged*, N.Y. TIMES (Oct. 24, 2017), https://nyti.ms/2zxSnXU [https://perma.cc/PBT8-ZV75] (explaining that Microsoft dropped its lawsuit in response to the government's new policy).

intermediaries to quite literally "copy[] the whole Internet" and turn it over to the government on a handshake agreement.[36] Then again, scholars who believe that surveillance intermediaries are well-positioned to challenge government overreach have good reason to be hopeful; the rise of intermediary-driven litigation post-Snowden demonstrates that technology companies can and will stand up for the privacy rights of their users. The trouble with the existing scholarship on surveillance intermediaries is that neither position is wrong — but by focusing on this assistance-versus-resistance dichotomy, scholars overlook the nuances in intermediary decisionmaking that illustrate their incentive structures.

One such nuance is that a single company's commitment to resistance against or cooperation with the government cannot be assumed to remain static over time. Consider, for example, the history of Western Union's relationship with the government: During World War II, Western Union sent copies of all international cables to U.S. intelligence agencies in a handshake agreement known as Operation Shamrock.[37] When the war ended, this program continued for another thirty years without any legal basis.[38] The 1976 Church Committee Report exposed this state of affairs,[39] among many other major privacy violations committed by U.S. intelligence agencies,[40] in a shocking moment of history quite similar to the Snowden revelations. Operation Shamrock came to an "abrupt end," and there is no indication that Western Union had any relationship with the U.S. government for decades after that.[41] But, in the wake of 9/11, Western Union again began working with the government, in a relationship that was characterized by "informal cooperation rather than legal compulsion."[42] Western Union customers may have thought that the company would never again enter into a questionable legal arrangement with the government after Operation Shamrock — but they would have been wrong.

Another nuance is that all surveillance intermediaries cannot be assumed to respond to any given circumstance in a uniform manner. While many companies may have tended to cooperate with the government after 9/11 and resist the government after Snowden, this trend is certainly not true for all surveillance intermediaries. Although some news outlets incorrectly reported that tech companies like Google and

---

[36] WU, *supra* note 11, at 249 (quoting Nakashima, *supra* note 19).

[37] Michaels, *supra* note 11, at 914.

[38] *See id.*

[39] S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 104 (1976).

[40] *See generally id.*

[41] Michaels, *supra* note 11, at 914.

[42] *Id.*

Facebook willingly gave intelligence agencies direct access to their users' data post-9/11, there is no evidence that this was the case.[43] In fact, at least some tech companies — including Yahoo and Twitter — challenged national security–related requests long before the Snowden disclosures.[44] Similarly, it is not true that all technology companies have become privacy advocates in the wake of the Snowden disclosures. In 2017, telecom companies successfully lobbied Congress to *remove* their privacy obligations to their customers.[45] Internet service providers such as Comcast and Verizon led this effort, and they received support from tech companies such as Facebook, Google, Twitter, and Amazon.[46]

Do technology companies facilitate or frustrate government surveillance? The answer is that they do both, and this fluctuation should give one pause. Reasonable minds may differ as to what the ideal balance between cooperation and resistance might be, but it seems unlikely that this balance should be left to the judgment of a private corporation.[47] Whatever the appropriate amount of cooperation — or resistance — is, this is an important public policy issue, and it should be decided with regard to the public's best interests and wishes. When creating regulations, it is critical to understand *why* surveillance intermediaries make the decision to resist or cooperate, and to attempt to align those incentive structures with a balanced approach to security and privacy.

B. Incentives Driving Surveillance Intermediary Behavior

In order to regulate the degree to which surveillance intermediaries resist or assist law enforcement, it is critical to understand what incentives they consider when deciding how to respond to a government request for information. Current scholarship on this issue focuses on how intermediaries have reacted to two major national events: 9/11 and the Snowden revelations.[48] While there is little doubt that these represent critical turning points in the behavior of surveillance intermediaries[49] —

---

[43] Ed Bott, *How Did Mainstream Media Get the NSA PRISM Story So Hopelessly Wrong?*, ZDNET (June 14, 2013, 5:09 AM), http://www.zdnet.com/article/how-did-mainstream-media-get-the-nsa-prism-story-so-hopelessly-wrong/ [https://perma.cc/LYQ7-N7RH].

[44] Claire Cain Miller, *Secret Court Ruling Put Tech Companies in Data Bind*, N.Y. TIMES (June 13, 2013), https://nyti.ms/19xeJIY [https://perma.cc/KQ7F-7JXX].

[45] Alex Byers, *How a Telecom-Tech Alliance Wiped Out FCC's Privacy Rules*, POLITICO (Mar. 31, 2017, 3:31 PM), https://www.politico.com/story/2017/03/broadband-data-victory-republicans-236760 [https://perma.cc/2525-7CQN].

[46] *See id.*; Ernesto Falcon, *How Silicon Valley's Dirty Tricks Helped Stall Broadband Privacy in California*, ELECTRONIC FRONTIER FOUND. (Oct. 23, 2017), https://www.eff.org/deeplinks/2017/10/how-silicon-valleys-dirty-tricks-helped-stall-broadband-privacy-california [https://perma.cc/F2JZ-53T5].

[47] This is not to say that tech companies do not *attempt* to strike the right balance given the power that they find themselves with. *See, e.g.*, Smith, *supra* note 26.

[48] *See supra* section A, pp. 1724–27.

[49] *See* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1116 (2016); Rozenshtein, *supra* note 7, at 104–05, 116–19.

and in our law enforcement and national security apparatus as a whole[50] — there are many other subtle incentive structures at play in intermediary decisionmaking. By teasing out a more complete picture of why surveillance intermediaries make decisions, we can see that intermediaries are not a monolith: each company is likely to assist and resist law enforcement agencies to different degrees and in different ways across varying situations and over time. This section reviews four major incentive structures driving intermediary behavior, but it is far from a complete list.

In addition to these incentives, it is important to note that, doctrinally speaking, the *only* valid purpose of a for-profit company incorporated in Delaware is to generate profits for its shareholders.[51] Most public surveillance intermediaries fall into this category.[52] Although this rule is more or less impossible to enforce, it is nonetheless the bedrock principle that is supposed to animate every decision made by corporations like Facebook and Google. While in practice companies may have a range of motivations, the profit motive can be seen as driving each of the incentives discussed below, at least in part. One might argue that this profit motive is not necessarily aligned with — if not fundamentally at odds with — the behavior one would hope to see from an entity expected to advocate for our privacy and civil liberties.

1. Current Events. — As the aftermaths of 9/11 and the Snowden revelations highlight, one major incentive in intermediary decisionmaking is reacting to current events, and particularly to public criticism of the intermediary.[53] When that event is something that affects *all* intermediaries, as 9/11 and the Snowden revelations did, we can perhaps expect many of them to react similarly: for example, as noted above,

---

[50] *See* Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1655, 1655–56 (2006); *see also* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004), http://govinfo.library.unt.edu/911/report/911Report.pdf [https://perma.cc/9GZM-5K5E].

[51] *See* eBay Domestic Holdings, Inc. v. Newmark, 16 A.3d 1, 34 (Del. Ch. 2010).

[52] *See, e.g.*, Facebook, Inc., Registration Statement (Form S-1) (Feb. 1, 2012) (denoting Facebook as a Delaware corporation); *see also* Juliette Garside, *Google's Alphabet Restructure Could Get Boost from Delaware Tax Loophole*, THE GUARDIAN (Aug. 11, 2015, 12:17 PM), https://www.theguardian.com/technology/2015/aug/11/google-alphabet-delaware-tax-loophole [https://perma.cc/KG7G-7XNT].

[53] It may be tempting to think that surveillance intermediaries reacting to the public outcry of end users in this way is a form of democracy that should be embraced. Rozenshtein provides a strong rebuttal to this argument:

> "[W]e shouldn't rely on surveillance intermediaries to cure any democratic deficits that may exist in surveillance policymaking. . . . Surveillance intermediaries often have idiosyncratic ideological views on surveillance. *The market does not provide a sufficiently precise incentive for surveillance intermediaries to bring government surveillance in line with popular preferences*. Surveillance intermediaries may use the opportunity to oppose government surveillance to generate trust that may ultimately prove unearned . . . ."

Rozenshtein, *supra* note 7, at 180 (emphasis added).

many surveillance intermediaries began resisting government requests for information after the Snowden revelations by bringing the government to court.[54]

However, there are often events or public criticisms that affect only a single company. When that happens, only that intermediary will be incentivized to adjust its behavior — for example, it might challenge a government action that other companies comply with.

Take, for instance, Google's reaction to the severe public criticism it faced in the 2000s for its relationship with China.[55] Google launched Google.cn in January 2006.[56] This Chinese version of its search engine openly complied with Chinese censorship laws,[57] "filter[ing out] keywords like 'human rights' and 'democracy,'"[58] and otherwise significantly limiting search results.[59] Media outlets and human rights organizations publicly condemned Google for this move; for example, the free speech advocacy group Reporters Without Borders stated "[t]he launch of Google.cn is a black day for freedom of expression in China."[60]

Just days before the launch of Google.cn, Google publicly refused to comply with a U.S. government subpoena for its users' search queries.[61] In an effort to prove the efficacy of the Child Online Protection Act, the government requested data on the search queries of millions of Google users.[62] Google refused to comply with the subpoena, on the grounds that it was "unnecessary, overly broad, would be onerous to comply with, would jeopardize its trade secrets and could expose identifying information about its users."[63] This resistance was partially successful: Google had to turn over some of the requested records, but not all.[64] In

---

[54] *See supra* section A, pp. 1726–27.

[55] *See* Peter Pollack, *Congress Grills Tech Firms over China Dealings*, ARS TECHNICA (Feb. 15, 2006, 11:51 PM), https://arstechnica.com/uncategorized/2006/02/6192/ [https://perma.cc/XU5W-KUP9].

[56] Andrew McLaughlin, *Google in China*, GOOGLE OFFICIAL BLOG (Jan. 27, 2006), https://googleblog.blogspot.com/2006/01/google-in-china.html [https://perma.cc/SAE5-RLQM].

[57] Anders Bylund, *Google Bows to Chinese Demands*, ARS TECHNICA (Jan. 25, 2006, 1:55 PM), https://arstechnica.com/uncategorized/2006/01/6051-2/ [https://perma.cc/QN2P-T6BZ].

[58] Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES (Jan. 20, 2006), https://nyti.ms/2vnwafZ [https://perma.cc/EC9G-X5M3].

[59] *See* Bylund, *supra* note 57.

[60] *Id.*

[61] *See* Hafner & Richtel, *supra* note 58 ("Google has been refusing the request since a subpoena was first issued last August . . . .").

[62] *Id.*

[63] *Id.*

[64] Eric Bangeman, *Google Will Have to Turn Over Search Data to the Government*, ARS TECHNICA (Mar. 14, 2006, 2:41 PM), https://arstechnica.com/uncategorized/2006/03/6381-2/ [https://perma.cc/NN59-QHMY].

Google's Transparency Report,[65] this episode is highlighted as the company's first big stand for transparency and user privacy.[66] As the Department of Justice noted in its response to Google's lawsuit, several other surveillance intermediaries — Microsoft, Yahoo, and AOL — complied with similar subpoenas without objection.[67]

The timing of Google.cn's launch and Google's first major stand for privacy in the United States did not go unnoticed. Many commentators suggested that Google decided to resist the U.S. government's subpoena in order to bolster its privacy credentials in the United States.[68] Here we see a surveillance intermediary making the decision to resist an overbroad government subpoena, likely at least in part due to negative publicity it received on a completely separate issue.

2. Technical Structure. — Another incentive relevant to intermediary decisionmaking is the technical structure of the company or the company's products. Intermediaries have made different technical design choices, which in turn impact their decisionmaking with regard to surveillance.

Consider Microsoft's successful challenge to a government search warrant for data stored abroad. In 2013, Microsoft refused to comply with a federal search warrant for a narcotics case in Manhattan.[69] The search warrant sought emails that Microsoft had stored on a server in Ireland.[70] As such, Microsoft insisted that it could not turn the data over to the U.S. government — to do so would violate the presumption against extraterritoriality.[71] The District Court sided with the government,[72] but the Second Circuit found in favor of Microsoft.[73] As a result, under Second Circuit law tech companies can no longer comply with U.S. search warrants that request data stored abroad — U.S. courts do not have the jurisdiction to authorize the search of such data, and the

---

[65] A transparency report discloses statistics about government requests for user data. *See, e.g.*, sources cited *supra* notes 1–4. For a list of companies that issue transparency reports, see *Transparency Reporting Index*, ACCESS NOW, https://www.accessnow.org/transparency-reporting-index/ [https://perma.cc/DB78-9JKF].

[66] *A History of Transparency*, GOOGLE: TRANSPARENCY REP., https://transparencyreport.google.com/about [https://perma.cc/5JCP-G3FJ] ("Google makes headlines for refusing a government request. . . . Google resists a Justice Department request to turn over records on millions of users' search queries. The request, enabled by the USA Patriot Act, is ostensibly part of the government's effort to uphold an online pornography law.").

[67] *See* Hafner & Richtel, *supra* note 58.

[68] Bylund, *supra* note 57; *see* Hafner & Richtel, *supra* note 58.

[69] Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 200 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (2017).

[70] *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014), *rev'd sub nom. Microsoft*, 829 F.3d 197, *cert. granted*, 138 S. Ct. 356.

[71] *Id.* at 468.

[72] *Id.* at 477.

[73] *Microsoft*, 829 F.3d at 222.

Stored Communications Act[74] does not allow tech companies to disclose content information without a valid legal request. The Supreme Court granted certiorari, and the case will be decided in 2018.[75]

Microsoft has made it clear that it is interested in pursuing impact litigation to preserve the privacy of its customers, and this case is one of its efforts to do so. But something that isn't quite so obvious is that Microsoft is uniquely situated to *comply* with the Second Circuit's decision. This is because Microsoft has a "regionalized" cloud system, with data centers located all over the world.[76] It makes an effort to store user data in a data center close to that person.[77] As a result, Microsoft employees can easily tell where in the world a specific piece of data is stored — if the government requests data located outside of the United States, they simply don't turn it over.

Other companies, such as Facebook and Google, have structured their clouds very differently. Although both companies have customers all over the world, neither has pursued a regionalized cloud model akin to Microsoft's.[78] Facebook has data centers in only three countries — the United States, Sweden, and Ireland[79] — and Google in only eight — the United States, Chile, Taiwan, Singapore, Ireland, the Netherlands, Finland, and Belgium.[80] As a result, data stored by both companies tends to be "pinging around a globally distributed network" to reach their users.[81] So when Facebook and Google comply with government requests for data, it is not so clear *where* in the world that data is coming from.[82] Compliance with the Second Circuit's ruling is therefore less straightforward for Facebook and Google than it is for Microsoft.

The lesson here is that we cannot assume that surveillance intermediaries are interchangeable in the lawsuits they choose to pursue — there is a reason why Microsoft is the company that pursued a case about

---

74 18 U.S.C. §§ 2701–2712 (2012).

75 *Microsoft*, 138 S. Ct. 356; United States v. Microsoft Corp., SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/ [https://perma.cc/DJ4Y-PLHY].

76 *Where Is My Data?*, MICROSOFT AZURE, http://o365datacentermap.azurewebsites.net/ [https://perma.cc/2FS7-QX6B].

77 *Id.*

78 Andrew Keane Woods, *Reactions to the Microsoft Warrant Case*, LAWFARE (July 15, 2016, 7:21 AM), https://www.lawfareblog.com/reactions-microsoft-warrant-case [https://perma.cc/RRV6-TRGV].

79 Nikolaj Skydsgaard, *Facebook to Build Third Foreign Data Center in Denmark*, REUTERS (Jan. 19, 2017, 4:14 AM), https://www.reuters.com/article/us-facebook-denmark/facebook-to-build-third-foreign-data-center-in-denmark-idUSKBN15310F [https://perma.cc/9WEB-NHY8]. Facebook will open its third foreign data center, located in Denmark, in 2020. Odense Data Ctr., *Odense Data Center Construction and Subcontracting Information*, FACEBOOK (June 28, 2017), https://www.facebook.com/notes/odense-data-center/odense-data-center-construction-and-subcontracting-information/1264865323635358/ [https://perma.cc/2V6R-PYHV].

80 *Data Center Locations*, GOOGLE, https://www.google.com/about/datacenters/inside/locations/index.html [https://perma.cc/EG66-FW3Z].

81 Woods, *supra* note 78.

82 *See id.*

extraterritoriality, and not Facebook or Google. Here, Microsoft asked the Second Circuit to make a rule that it knew it would be able to comply with under its regionalized cloud system. Companies with nonregionalized cloud systems, like Facebook and Google, would *not* have brought this case to court, because they would have been asking for a rule that presents a technical difficulty for them. In this way, the technical design of intermediaries and their products dictates, at least to some extent, what kind of law enforcement requests they might challenge in the first place.

3. Business Model. — A third incentive behind intermediary decisionmaking lies in the business model of each company. A surveillance intermediary will be incentivized to act in a way that promotes its own business model — and, better yet, a way that distinguishes its business model from that of its competitors.

Consider Apple's 2016 challenges to the government's use of the All Writs Act to compel Apple's assistance in unlocking iPhones for two government investigations. Because Apple encrypts all iPhone data, unlocking an iPhone is the only expedient way for the government to gain access to its contents.[83] The All Writs Act is used to "fill[] gaps where Congress has been silent," allowing a court to issue writs it "might need to effectuate its judgments."[84] By 2016, Apple had complied with such writs at least seventy times in the past.[85] Nonetheless, it successfully challenged the use of the All Writs Act in the Eastern District of New York for a narcotics case,[86] and it brought another such challenge in the Central District of California for a terrorism case.[87] Although Apple's challenge in the Central District of California was cut short when the government obtained an alternate means of unlocking the iPhone in

---

[83] *See* Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), https://nyti.ms/2k6dw48 [https://perma.cc/J6GH-VRZY].

[84] Rozenshtein, *supra* note 7, at 126.

[85] *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 346 (E.D.N.Y. 2016).

[86] *Id.* at 344.

[87] Apple Inc.'s Reply to Government's Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, *supra* note 33.

question,[88] the case generated significant publicity[89] and started a nationwide conversation about the balance between privacy and security.[90] In the midst of this resistance, Apple released a public letter to its customers emphasizing the importance of strong encryption.[91]

Apple's decision to resist the All Writs Act so publicly served to highlight an iPhone feature that differentiates Apple from many of its peers: the use of encryption so strong that even Apple cannot access its users' devices. Data security through strong encryption is central to Apple's business model.[92] This is in stark contrast to many other Silicon Valley companies, which primarily generate profit by analyzing and selling their users' data — in order to do that, these companies *cannot* block their own access to user data through encryption.[93] Tim Cook, Apple's CEO, has publicly criticized this alternative business model in the past: "They're gobbling up everything they can learn about you and trying to monetize it. We think that's wrong. And it's not the kind of company that Apple wants to be."[94] Apple's resistance to the All Writs Act was therefore likely motivated by its desire to differentiate itself from its peers.

4. Interests of Corporate and Individual Users. — Finally, surveillance intermediaries may react differently to the concerns of individual users and corporate users — especially when individuals use a free ver-

---

[88] Ellen Nakashima, *Once Again, the Government Finds a Way to Crack an iPhone Without Apple's Help*, WASH. POST (Apr. 23, 2016), http://wapo.st/1SAp3EM [https://perma.cc/6WQ9-MRVC].

[89] This is in no small part due to Apple's direct appeal to its customers. *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/7BY4-4TCU] ("The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake."); *see also* Julia Greenberg, *To Fight the FBI, Apple Ditched Secrecy for Openness*, WIRED (Mar. 25, 2016, 7:00 AM), https://www.wired.com/2016/03/fight-fbi-apple-ditched-secrecy-openness/ [https://perma.cc/MA4L-MMTF] ("Apple loves a show.").

[90] This conversation was so significant that the Pew Research Center conducted a poll on it. *See More Support for Justice Department than for Apple in Dispute over Unlocking iPhone*, PEW RES. CTR. (Feb. 22, 2016), http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/ [https://perma.cc/92AY-WBSU].

[91] *See* Cook, *supra* note 89.

[92] Lev Grossman, *Inside Apple CEO Tim Cook's Fight with the FBI*, TIME (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/ [https://perma.cc/V7FN-5ANV] ("[Apple CEO Tim] Cook is fond of pointing out that Apple's business model doesn't involve harvesting and mining its users' data the way that, say, Google, Facebook and Amazon do.").

[93] *Id.*

[94] Lily Hay Newman, *Tim Cook Says Apple "Doesn't Want Your Data." Let's Not Say Things We Can't Take Back*, SLATE: FUTURE TENSE (June 3, 2015, 5:49 PM), http://www.slate.com/blogs/future_tense/2015/06/03/tim_cook_s_pro_privacy_keynote_speech_at_the_epic_champions_of_freedom_event.html [https://perma.cc/S7VY-2VGM].

sion of their product and corporations use a paid version. Because corporate users often generate more revenue for an intermediary and have significant bargaining power when purchasing an enterprise version of the intermediary's product, their concerns are more likely to be heard over the concerns of individual users.

Take, for example, Google's summer 2017 announcement that it would stop scanning the contents of Gmail messages to generate targeted advertisements.[95] Privacy advocates and individuals had been sharply criticizing Google for this practice since Gmail launched in 2004,[96] but Google continued to engage in email scanning for thirteen years. According to journalists and privacy advocates, Google's change of heart did not occur in response to the decades-long objection of individual users.[97] Rather, Google was responding to the discomfort of its corporate users.[98] Although Google insisted that its enterprise product, G Suite, did not scan email contents for advertising purposes, corporate users remained uncomfortable with the notion that Google scanned the contents of Gmail messages at all.[99] In order to assuage these fears, Google decided to stop scanning Gmail across the board, in a move that reflected "Google's seriousness in winning over corporate customers."[100]

Although this example was not generated in response to a government subpoena, it is easy to see how this behavior carries over to Google's role as a surveillance intermediary. Further, Google's decision reflects how corporations react differently to individual versus corporate user privacy concerns. It is also important to note that this individual-versus-corporate user dynamic does not exist for every surveillance intermediary: while companies like Google and Apple work with both individuals and corporate users, and may be incentivized to behave differently when presented with the concerns of one class of user over another, other intermediaries, such as Facebook and Twitter, have primarily individual users.

---

95 Daisuke Wakabayashi, *Google Will No Longer Scan Gmail for Ad Targeting*, N.Y. TIMES (June 23, 2017), https://nyti.ms/2tYPWdW [https://perma.cc/N9BD-ZYHS]. Gmail will continue to feature targeted advertisements based on information collected from other sources, such as browsing history. *See id.*

96 *Id.*; *see also* Dominic Rushe, *Google: Don't Expect Privacy when Sending to Gmail*, THE GUARDIAN (Aug. 15, 2013, 3:00 AM), https://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit [https://perma.cc/L4VU-287B].

97 *See* Wakabayashi, *supra* note 95; Laurel Wamsley, *Google Says It Will No Longer Read Users' Emails to Sell Targeted Ads*, NPR (June 26, 2017, 5:40 PM), https://www.npr.org/sections/thetwo-way/2017/06/26/534451513/google-says-it-will-no-longer-read-users-emails-to-sell-targeted-ads [https://perma.cc/29BW-LZ3J].

98 *See* Wakabayashi, *supra* note 95; Wamsley, *supra* note 97.

99 *See* Wakabayashi, *supra* note 95.

100 *Id.*

C. The Advantages of Surveillance Intermediaries

The surveillance intermediary model is not perfect, particularly when it comes to the lack of consistent alignment between intermediary decisionmaking and the public interest. However, there are a number of positive institutional features of this system that might lead us to *want* large technology companies to act as our surveillance intermediaries. If regulatory authorities can navigate the complex web of incentives governing intermediary decisionmaking, the surveillance intermediary system can be leveraged to improve both the efficacy of legal protections for individual privacy and the efficiency of processing lawful requests for information.

Consider, for example, Microsoft's 2016 lawsuit against the U.S. government.[101] Microsoft alleged that the government routinely attached secrecy orders to search warrants and other requests for information, often for an indefinite amount of time, even when the facts of a case did not support the need for secrecy.[102] As a result, Microsoft was compelled to turn over user information to the government but was not able to notify its users when it did so. Microsoft claimed that the routine use of indefinite secrecy orders violated its customers' Fourth Amendment rights and Microsoft's own First Amendment rights.[103] In October 2017, the Department of Justice issued new secrecy order guidelines for U.S. Attorneys' Offices.[104] According to Brad Smith, Microsoft's President and Chief Legal Officer, the new policy "helps ensure that secrecy orders are used only when necessary and for defined periods of time."[105] Microsoft then dropped its lawsuit, but Smith assured its users that it would continue fighting for their privacy rights:

> We applaud the Department of Justice for taking these steps, but that doesn't mean we're done with our work to improve the use of secrecy orders. We have been advocating for our customers before the DOJ for a long time, and we'll continue to do that. We will continue to turn to the courts if needed. And we are committed to working with Congress.[106]

---

101 First Amended Complaint for Declaratory Judgment, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 2:16-cv-00538).

102 *Id.* at 3; Brad Smith, *Keeping Secrecy the Exception, Not the Rule: An Issue for Both Consumers and Businesses*, MICROSOFT: MICROSOFT ON THE ISSUES (Apr. 14, 2016), https://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/ [https://perma.cc/JKA2-4AU2].

103 First Amended Complaint for Declaratory Judgment, *supra* note 101, at 2.

104 Memorandum from Rod J. Rosenstein, *supra* note 35.

105 Brad Smith, *DOJ Acts to Curb the Overuse of Secrecy Orders. Now It's Congress' Turn.*, MICROSOFT: MICROSOFT ON THE ISSUES (Oct. 23, 2017), https://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn/ [https://perma.cc/E7PE-XDSV].

106 *Id.*

This lawsuit and the resulting policy change are an example of surveillance intermediaries at their best: Microsoft noticed a pattern of the government overusing secrecy orders and mobilized its considerable resources to change this practice. What's more, it did so of its own volition — indeed, a critical issue with the government's use of secrecy orders was the fact that the public could not know how often they were used without Microsoft cluing us in.

This case reflects a number of positive aspects of the surveillance intermediary system. First, the existence of surveillance intermediaries between the government and end users is a helpful mechanism for our legal system: "[W]hen surveillance intermediaries resist government surveillance, they . . . amplify[] the ability of Congress and the courts to regulate the surveillance state."[107] This is a point that a range of commentators seem to agree on, including former government attorneys most concerned with public safety[108] and scholars focused on protecting privacy and civil liberties.[109] Technology companies are able to generate public information about the Executive's surveillance programs, ensuring that all members of Congress are informed about law enforcement activities.[110] They can also demand court orders before complying with law enforcement requests for information, "put[ting] more and more . . . surveillance activity before the courts."[111] In short, surveillance intermediaries have the power to strengthen and reinforce the oversight power of Congress and the judiciary in the realm of the Executive's surveillance programs.[112]

Second, and relatedly, technology companies almost certainly know more about law enforcement requests for information than any other entity — including the government. Companies like Facebook, Google, and Twitter receive court orders from federal, state, and local governments. They can learn the idiosyncrasies of different offices, differentiate "normal" requests from aberrant ones, and identify concerning patterns. Indeed, even on the federal level there is room for a range of behavior from judges and U.S. Attorneys' Offices across the country.[113] No single organization has as large and clear a window into surveillance

---

107 Rozenshtein, *supra* note 7, at 150.

108 *E.g.*, *id.* at 99.

109 *E.g.*, Michaels, *supra* note 11, at 906 (writing in 2008, long before the Snowden revelations, and proposing to "flip the private-public partnerships on their heads, converting the privatization schemes from the handmaidens of inscrutable intelligence policy into the guarantors of a new counterterrorism regime built on legality, legitimacy, and accountability").

110 *See* Rozenshtein, *supra* note 7, at 152 ("Congress can't oversee government surveillance it doesn't know about." (citing David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 300–01 (2010))).

111 *Id.* at 154.

112 This is a positive development, because, as Rozenshtein notes, scholars have recently questioned whether "Congress and the courts have the necessary means and motives to police government surveillance." *Id.* at 150.

113 *See, e.g.*, Marimow & Timberg, *supra* note 8.

trends as these technology companies, and therefore no other organization is better positioned to respond to these trends.[114]

Third, technology companies are better situated to pursue surveillance-related litigation than any individual. There are a number of reasons why it is unlikely that any one person would be able to successfully sue the government over routine subpoenas and search warrants: At the outset, there are significant standing issues that might render such a suit impossible in the first place.[115] Further, individuals simply do not know enough about the degree and manner in which their personal data is collected by the government.[116] Finally, individuals are unlikely to have the resources to pursue effective litigation against the government.[117] In contrast, technology companies have the standing, knowledge, and resources required to challenge government orders when necessary.

Fourth, large technology companies have the resources to invest in robust policy teams that can devote themselves to evaluating the validity of law enforcement requests for information, responding to emergencies, and developing long-term litigation strategies when necessary. To take an example from outside of the surveillance context, consider the approach that companies such as YouTube, Facebook, and Twitter have taken to preserving freedom of speech online.[118] Despite the fact that these platforms have broad immunity from liability for user-generated content,[119] they each go through enormous effort and employ thousands of people in order to preserve free speech norms for their users to the greatest extent possible.[120] This is an example of the good-faith effort technology companies put into their work as private institutions with quasi-public functions — at the same time, this *is* a project motivated by "the necessity [to meet] users' norms for *economic viability*."[121]

---

[114] Many companies have taken steps to make at least some of this information public. *See Transparency Reporting Index*, *supra* note 65.

[115] *See* Rozenshtein, *supra* note 7, at 156–57; *see also infra* ch. II, pp. 1748–52.

[116] *Contra* Zakharov v. Russia, App. No. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, ¶ 179 (Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324 [https://perma.cc/PQ25-9XR7] (holding that an individual can challenge government surveillance in the absence of concrete proof that he has been under surveillance if "he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such [surveillance]," ¶ 171).

[117] In addition, the Stored Communications Act "lacks a statutory suppression remedy" — even if an individual managed to navigate the hurdles listed above, those seeking the suppression of evidence would be out of luck. Rozenshtein, *supra* note 7, at 155 (citing Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 806–07 (2003)).

[118] *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

[119] *Id.* at 1604.

[120] *Id.* at 1618–22.

[121] *Id.* at 1618 (emphasis added).

Finally, the existence of large technology companies as surveillance intermediaries is an enormous benefit to law enforcement agencies.[122] The evidence from these companies is often incredibly important to criminal cases and national security investigations,[123] and being able to turn to a small number of well-organized companies is critical to the efficiency and success of those pursuits.[124] While some have taken this to be a negative — that the Facebooks of the world make it all too easy for the government to slip into a dystopian Big Brother–esque surveillance state[125] — there are many reasons to consider this benefit for law enforcement agencies to be a benefit to the public. Data held by surveillance intermediaries has been indispensable to cases relating to terrorism, murder, and other serious crimes.[126] This information can be acquired in a cost- and time-efficient way when surveillance intermediaries have invested in an infrastructure for responding to court orders.

By providing a degree of transparency to government requests[127] and making independent assessments of their legality,[128] surveillance intermediaries can provide a valuable backstop to the Executive's law enforcement powers and set a *ceiling* on government overreach. At the same time, by providing clear law enforcement guidelines,[129] proactively assisting law enforcement with certain investigations,[130] and expediting responses to urgent requests,[131] intermediaries are also able to set a *floor*

---

122 *See, e.g.*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 1 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/U2KZ-LGMC] (describing law enforcement communities' concern that inability to access communications from technology companies will hinder the prevention of terrorism and crime prosecution).

123 *See id.*

124 *See id.* Consider also that many large technology companies make the request process as easy as possible for law enforcement agencies by creating dedicated web portals for them. *See, e.g.*, *Law Enforcement Online Requests*, FACEBOOK, https://www.facebook.com/records/x/login [https://perma.cc/9YB3-YQTM].

125 *See* WU, *supra* note 11, at 249; Schneier, *supra* note 11.

126 *See Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (2015), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf [https://perma.cc/6M96-TARQ] (written statement of New York County District Attorney Cyrus R. Vance, Jr.); BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD UNIV., *supra* note 122, at 1.

127 *See, e.g.*, *Transparency Reporting Index*, *supra* note 65; *cf.* Michaels, *supra* note 11, at 952 (advocating for corporate disclosure of information-sharing agreements with government actors).

128 *See* Michaels, *supra* note 11, at 951 (advocating for a requirement that corporations independently assess the legality of government requests for information).

129 *See, e.g.*, APPLE INC., LEGAL PROCESS GUIDELINES (n.d.), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/XPF2-2QHT]; *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines [https://perma.cc/S9CG-FD5V]; *Guidelines for Law Enforcement*, TWITTER, https://support.twitter.com/articles/41949 [https://perma.cc/YLB7-CUYY].

130 *See* Olivia Solon, *Facebook, Twitter, Google and Microsoft Team Up to Tackle Extremist Content*, THE GUARDIAN (Dec. 5, 2016, 8:47 PM), https://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content [https://perma.cc/B584-SYU4].

131 *See* sources cited *supra* note 129.

of assistance that law enforcement officials can expect from technology companies. Setting a ceiling and floor for compliance with government requests for information is an incredibly valuable role for surveillance intermediaries to play — and technology companies are well equipped to do it.

D. Conclusion

Surveillance intermediaries are not a monolith. This is an umbrella term that encompasses a wide range of companies with different user bases, business models, income streams, and public relations strategies. Surveillance intermediaries play a significant role in our law enforcement and national security apparatus, and their behavior in that role varies significantly over time and between companies. As Congress and our courts move toward regulating large technology companies, they would do well to understand the complex web of incentives that govern intermediary behavior. If they are able to do so, we can harness the resources and insight of intermediaries for the public good. If they fail to do so, however, and instead subscribe to the belief that intermediaries tend to either resist or assist the government, they will miss the important nuances driving intermediary behavior.