Brooklyn Law Review

Volume 82 | Issue 1 Article 3

Fall 12-1-2016

Governance by Proxy: Cyber Challenges to Civil Liberties

Niva Elkin-Koren

Eldar Haber

Governance by Proxy

CYBER CHALLENGES TO CIVIL LIBERTIES

Niva Elkin-Koren[†] *& Eldar Haber*[††]

INTRODUCTION

The greatest challenges we are likely to face in the information environment over the next decade are challenges to civil liberties. For a long time, members of society in liberal democracies have taken civil liberties for granted, as they have been reasonably secured by well-established constitutional principles, the separation of powers, and a bill of rights. Recent developments suggest, however, that those checks and balances may no longer be sufficient to secure civil liberties in the years to come.

One reason for the risk to civil liberties is a governance crisis, which gives rise to new types of collaboration between governments and online intermediaries in managing online behavior. The distributed nature of Internet architecture shifted power from traditional governing institutions to individual users.[1] End users can mass communicate content,[2] raise significant funds, create and share economic value, and engage in political action, thereby bypassing mass media, firms, and political parties.[3] The distributed nature of the Internet, at the initial stages of its development, shifted power from traditional institutions to end users, acting alone or in collaboration with

[†] Professor of Law, University of Haifa, Faculty of Law; Director, Haifa Center for Law & Technology, University of Haifa, Faculty of Law.

[††] Assistant Professor, University of Haifa, Faculty of Law; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University. This research was funded by the Israeli Ministry of Science, Technology and Space (MOST).

[1] Yochai Benkler, *Degrees of Freedom, Dimensions of Power*, 145 DAEDELUS 18, 19–20 (2016).

[2] *See* MANUEL CASTELLS, COMMUNICATION POWER xix (2013).

[3] *See generally* CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS (2008) (arguing that the advent of online social tools has reduced the transaction cost of collaboration, and enabled individual users to act together without needing to rely on traditional institutions).

others.[4] From the perspective of governments, this shift has created a governance challenge; how does the government ensure public safety, secure critical infrastructure, and safeguard national security in an era of open communication networks?

In order to address these issues, governments increasingly rely on informal collaboration with the private sector in cybersecurity, surveillance, censorship, and general law enforcement tasks. PRISM—a surveillance program of the National Security Agency (NSA)—is a classic example of surveillance and data sharing between online intermediaries and government agencies.[5] Under PRISM, the NSA targeted the contents of communications from nine major U.S. Internet companies through, inter alia, a partnership.[6] In other cases, intermediaries complied with informal calls to remove content or block access to websites or users.[7]

The revelations of Edward Snowden in 2013 regarding numerous surveillance programs like PRISM,[8] which were conducted by governmental agencies, should have been a wakeup call to the general public on how informal collaboration between online intermediaries and the government could turn the Internet into a robust system of surveillance and control. Overall, the Snowden revelations demonstrated the deep crisis of safeguarding civil liberties in liberal democracies. The NSA surveillance programs[9] provoked some litigation and legislative initiatives challenging the legality of these surveillance practices and the extent to which they comply with constitutional safeguards.[10] The recently enacted Cybersecurity Act of 2015 (Cybersecurity Act) sought to remedy some of these concerns following a series of subsequent governmental reports.[11]

So far, however, the legal initiatives of policymakers in the post-Snowden era have overlooked the innovative

---

[4] *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); William H. Dutton, *The Fifth Estate Emerging Through the Network of Networks*, 27 PROMETHEUS 1, 2 (2009).

[5] *See infra* Part I.

[6] *See infra* Part II.

[7] Angela Daly, *Private Power and New Media: The Case of the Corporate Suppression of WikiLeaks and Its Implications for the Exercise of Fundamental Rights on the Internet*, *in* HUMAN RIGHTS AND RISKS IN THE DIGITAL ERA: GLOBALIZATION AND THE EFFECTS OF INFORMATION TECHNOLOGIES 81 (Christina M. Akrivopoulou & Nicolaos Garipidis eds., 2012); *see, e.g.*, *infra* note 44.

[8] *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/5XF4-PUXZ].

[9] *See infra* Section II.A.

[10] *See infra* Section IV.B.

[11] *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015) (codified at 6 U.S.C. §§ 1501–1510 (2012)).

governance structure typical of online government practices. The Snowden revelations placed a spotlight on an intriguing public-private partnership (PPP). In a typical PPP, a public government entity, who is otherwise constitutionally restricted in its ability to search through electronic data of users, requests that the private entity do the actual searching and pass on certain types of information. Informal PPPs enable governments to bypass constitutional constraints because private bodies are not subject to constitutional limits on search or censorship and are under no duty to respect free speech or other fundamental rights.[12] Intermediaries are often offered immunity from civil lawsuits by users whose interests were compromised by an intermediary's action or inaction.[13] Consequently, citizens could be left without any remedy as a result of the nature of these PPPs. In the absence of any mechanisms to hold governments and intermediaries accountable, informal PPPs pose a new type of threat to civil liberties.

This emerging form of governance partnership between the state and the private sector raises new challenges. A decade ago, one of the authors warned that the regulatory framework in the post-9/11 era may facilitate this type of informal collaboration, termed the *invisible handshake,* between the state and the private sector.[14] The Snowden revelations showed that this new type of PPP is even broader than predicted. They further stressed challenges involved in bringing this type of practice under the rule of law. While the post-Snowden era has presumably brought the PPP between the government and online intermediaries to light, the PPP essentially remains as invisible as before because the details of its operation remain unknown. More importantly, the new type of collaboration between government and online intermediaries in governance evades the rule of law. It is executed in a *regulatory twilight zone*, which keeps this type of collaboration beyond the reach of constitutional law and outside the reach of the market powers that could push back against it.

What is the future of such alliances? It is not clear, as secrecy played a crucial role in the success of the PPP. What is most intriguing in the post-Snowden era is that the exposure of

---

[12] *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 1, 55 (2003).

[13] *See infra* Section II.B.

[14] Michael Birnhack and Niva Elkin-Koren coined this form of public-private partnership as the "invisible handshake," warning that such handshake could persist under the current regulatory framework without proper checks and balances. *See* Birnhack & Elkin-Koren, *supra* note 12, at 6.

PPPs did not prompt social or market powers to cease them, but instead led to their formal incorporation into law.[15] Consequently, PPPs are now encouraged by the law through incentives, but remain invisible to the public as before. In other words, not only did Snowden's revelations fail to increase protection of freedom and liberties, they led to an even more robust, and now legalized, system of surveillance.

This article scrutinizes the *governance by proxy* that occurs under the new type of PPP and the legal twilight zone that facilitates it. It identifies the gaps in the law and offers some insights on how to address them. Part I introduces the governance crisis and describes the role of online intermediaries in the new governance models, focusing on the case of PRISM. Part II describes the legal twilight zone in which informal governance by intermediaries takes place. It compares the legal framework for PPPs prior to the information era with the legal regime that facilitated the rise of PRISM. Part III reviews the constitutional and statutory frameworks that facilitate the invisible handshake and examines it from the perspective of both the government and online intermediaries as state actors. Part IV evaluates potential social and legal interventions that might be necessary to protect liberty and freedom and suggests turning to organizational design to significantly improve such protection. Ultimately, this article calls for a restructuring of the legal regime that governs PPPs.

I. THE PUBLIC PRIVATE HANDSHAKE: GOVERNANCE VIA ONLINE INTERMEDIARIES

A. The Governance Crisis

The Internet shifted power from central institutions (e.g., governments), organizations (e.g., mass media), and design infrastructure (e.g., mainframe) to end-users. Internet architecture enabled any end user to tinker with systems, change its design, directly connect with another, create content, and share content without filtering. The distributed architecture of the Internet raised high hopes for transforming fundamental economic structures and enabling new levels of political freedom.[16] It made it possible for individuals to connect, collaborate, share, deliberate, and act together efficiently and effectively.[17] It

---

[15] *See* Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2935, 2935–56 (2015) (codified at 6 U.S.C. §§ 1501–1510 (2012)).

[16] *See generally* BENKLER, *supra* note 4.

[17] *See generally id.*

facilitated mass communication by individuals on a scale that was once the sole province of mass media.[18] Individuals now use social media to engage in ad hoc political action: filing online petitions, recruiting supporters, and organizing street protests and boycotts. The dispersed wisdom of strangers gives crowds the advantage of political power capable of responding quickly and authentically to ongoing challenges. In this sense, online crowds could be thought of as a "*fifth estate*,"[19] supplementing mass media (the "*fourth estate*") and remedying its commercial and political biases. They could act as a counterforce, capable of pushing against the misuse of power and improving government accountability.

All in all, the distributed nature of the Internet has many virtues. It is responsible for the greatest benefits of the Internet: flourishing innovation, democratization of education, access to knowledge, political participation by many, and the export of democratic values from liberal democracies to non-democratic regions. But the unmediated nature of the Internet, which gave rise to the innovation burst, economic flourishing, and political aphorism, has also created a governance crisis. It has challenged the conventional way of governance and has introduced new types of threats.

The decentralized nature of the Internet makes systems and individuals more vulnerable and leads to greater risks. As society becomes more connected to, and dependent upon, instant, online access to services, it becomes necessary to offer security not only to critical infrastructure, but also to small- and medium-sized businesses, and to individual users. Security specialists are concerned that cyberspace could make it easier for extremists and terrorists to conceal their identities and actions, to reach out to their supporters, and to communicate with one another more efficiently than before.[20] Governments must protect against these risks—risks to the integrity of their data and the functionality of their systems, and risks to public safety and national security.

---

[18] *See* CASTELLS, *supra* note 2, at xix–xv.

[19] Dutton, *supra* note 4. The historical conception of feudal societies was traditionally divided into three "estates of the realm." *See* KAREN ORREN, BELATED FEUDALISM: LABOR, THE LAW AND LIBERAL DEVELOPMENT IN THE UNITED STATES 6 (1991). The fifth estate could take various forms. Relating to the Internet, Stephen Cooper argued that bloggers are the fifth estate, while William Dutton argued that any networked individuals—not just bloggers—are the fifth estate. *See generally* STEPHEN D. COOPER, WATCHING THE WATCHDOG: BLOGGERS AS THE FIFTH ESTATE (2006); Dutton, *supra* note 4.

[20] RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 71 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/9ZAB-PGUL].

Digital networks are in many ways a disruptive technology for the state. An open network, where power lies with the users at the end nodes, is inconsistent with the fundamental principles of command and control.[21] When individual users have the potential power to cause significant harm, law enforcement agencies seek ways to predict threats, prepare for them, and prevent them ahead of time. If every user can share information online, without any filtering, how can governments stop the sharing of data that harms individual privacy? How can governments stop the distribution of malware, detect those who incite violence, or identify calls for political unrest? The standard measures of governance are losing power.

The nature of cyber threats is dispersed. Many times, cyber attacks are difficult and expensive to detect[22] and to attribute to a specific attacker.[23] Illegal behavior might still be expensive and difficult to track when conducted by massive numbers of users.[24] Even if authorities are able to determine the actor of a cyber threat, the threat might originate from individuals outside their jurisdiction. This could make it difficult to track potential offenders or bring them to trial.[25]

---

[21] *See, e.g.*, Julia Black, *Critical Reflections on Regulation*, 27 AUSTL. J. LEG. PHIL. 1, 2 (2002). Such form of regulation usually refers to state regulation using legal rules backed by sanctions.

[22] Detection, in many instances, will usually occur only after a successful attack, while the attacker can conduct endless attempts until successful. This is highly different from many other types of crimes or acts of terror. Usually, committing crimes and acts of terrorism necessitate risk of detection. Therefore, in cyberattacks, the attacker has a very high probability of success (because if he does not succeed, he will not be sanctioned), which highly impacts the potential deterrent effect. For a similar argument, see Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 451 (2012). Moreover, in many instances, even if disruption in digital networks is discovered, it will not be clear whether the disruption was caused by an attack or a malfunction. *See* PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 18 (1997) ("Computer intrusions do not announce their presence the way a bomb does. . . . It sometimes takes months, even years, to determine the significance of individual computer attacks.").

[23] Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1536 (2010) (stating that "thousands of companies" are victims of cyberattacks but "the companies do not even know they are compromised until law enforcement authorities tell them"); Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 330 (2013) ("Cyber events are difficult to predict, plan for, and identify.").

[24] *See* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 66 (2001) ("Law enforcement resources in cyberspace cannot keep pace with sophisticated cybercrime subcultures in anonymous offshore havens.").

[25] When an attack occurs from beyond the physical borders of the state, then it could have various ramifications in terms of enforcement and jurisdiction. It generally becomes difficult to decide what happened where and enforcement is more difficult. For more on the meaning of physical and digital borders in "cyberspace" (referring to the

Crowdfunding online, and the ability to raise and transfer funds anonymously outside the banking system, poses yet another challenge for the enforcement agencies, due to its anonymized nature.[26] Ad hoc groups often lack a sustainable organizational structure, which makes it difficult to monitor them and restrain their illegal activities.[27] In the absence of a formal organizational structure, law enforcement agencies must identify individually each and every actor in a potentially illicit behavior. Online crowds are also more difficult to deter. Unlike repeat players, such as firms, political parties, or non-governmental organizations (NGOs), ad hoc crowds lack long-term interests and therefore risk management is less likely to play a mitigating role. Therefore, ad hoc crowds are less likely to respond to monetary sanctions.

Overall, users acting online, either alone or in collaboration, without any formal organizational structure are difficult to govern. The existence of potentially powerful tools in the hands of users may require law enforcement agencies to monitor each user. It is not a question of whether bulk surveillance will aid the government in protecting national security or merely reduce that risk at the margin.[28] It is mostly a question of governance; law enforcement efforts cannot rely on existing institutions or organizational structures.

Governments have reacted to this governance crisis in various ways. Some states have pushed for more centralized

---

Internet) see David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521 (2003). *See also* LAWRENCE LESSIG, CODE: VERSION 2.0 23–24 (2006) (arguing that controlling commercial online gambling is much more problematic in the online environment than in the physical world, mainly because of jurisdiction); Kesan & Hayes, *supra* note 22, at 454 (discussing the difficulties in determining whether the state acquired jurisdiction).

[26] *See generally* JEAN-LOUP RICHET, U.N. OFFICE ON DRUG & CRIME, LAUNDERING MONEY ONLINE: A REVIEW OF CYBERCRIMINALS' METHODS (2013), http:// arxiv. org/abs/1310.2368 [https://perma.cc/3E4L-U2XL] (describing methods that criminals use to launder money online).

[27] TAYLOR OWEN, DISRUPTIVE POWER: THE CRISIS OF THE STATE IN THE DIGITAL AGE 93–94 (2015).

[28] In programs conducted under section 215 of the USA PATRIOT Act, the NSA reported that they disrupted fifty-four terrorist incidents. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–90 (2001) (codified at 50 U.S.C. §§ 1861–1862); Ellen Nakashima, *NSA Cites Case as Success of Phone Data-Collection Program*, WASH. POST (Aug. 8, 2013), http://www.washingtonpost. com/world/nationalsecurity/nsa-cites-case-as-success-of-phone-data-collection-program/2013/ 08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html [https://perma.cc/N4WK-Q35E]. Other reports suggest lower numbers. *See Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 9 (2013) (statement of John C. Inglis, Deputy Dir., Nat'l. Sec. Agency, stating that the program helped in about twelve of thirteen cases).

control over the Internet. For instance, as a backlash to the Snowden revelations, countries such as Russia and Brazil announced plans to nationalize Internet infrastructure.[29] Other countries, like the United States, reacted to these new governance challenges by implementing innovative governance strategies.[30] These new governance strategies may include the use of mass surveillance and big data analysis to monitor potential risks, the use of algorithms in law enforcement efforts,[31] and the involvement of online intermediaries in governance efforts. These strategies challenge traditional thinking about safeguards for civil rights. Basically, this new approach to Internet governance takes advantage of the network—and employs network strategies—to secure public safety, cybersecurity, and law enforcement.

B. Governance via Online Intermediaries

Economies of scale led to the domination of online services by a small number of multinational mega platforms.[32] Online access, distribution, and exchange are hosted, facilitated, and mediated by a variety of online platforms such as Internet Services Providers, search engines (e.g., Google, Yahoo!), social media platforms (e.g., Facebook, Twitter), or hosting services (e.g., Apple, Amazon, YouTube). Online platforms have experienced a high level of growth, consolidation, and market concentration. Largely, this growth can be attributed to the fact that much of the costs of producing these platforms "is unrelated to the number of users of the service, [and thus] the average cost of providing service to each additional user may fall as the number of users increases."[33] But economies of scale reduce the level of competition. Cost of entry is rapidly rising as the Internet continues to grow and as competition becomes more sophisticated.[34] A strong network effect gives advantages to large-scale intermediaries, such as Google's search engine, and

---

[29] *See* Amanda Holpuch, *Brazil's Controversial Plan to Extricate the Internet from US Control*, GUARDIAN (Sept. 20, 2013), http://www.theguardian.com/world/2013/sep/20/brazil-dilma-rousseff-internet-us-control [https://perma.cc/2J5M-2H7N].

[30] *See infra* Part II.

[31] Algorithmic law enforcement becomes prevalent for detecting illicit behavior, for removing harmful materials, blocking access, or disabling the risk. Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. (forthcoming 2016).

[32] NIVA ELKIN-KOREN & ELI M. SALZBERGER, THE LAW AND ECONOMICS OF INTELLECTUAL PROPERTY IN THE DIGITAL AGE: THE LIMITS OF ANALYSIS 170 (2013).

[33] *Id.*

[34] *See* Directorate Gen. for Internal Policies, Policy Dep't, Econ. & Sci. Policy, *Presentation: Challenges for Competition Policy in a Digitalised Economy*, at 25, IP/A/Econ/2014-12 (July 2015).

to global social networks, such as Facebook, which currently attract the most traffic by users on a global scale.[35] Consequently, a handful of online intermediaries dominate the access to content, people, and communication infrastructure in the digital ecosystem.

Online intermediaries exercise control over *content* (as publishers of applications and media content), *access* and *distribution channels*, and, finally, *end users' personal data* and *devices* (e.g., Kindle, iPhone). By establishing direct contact with each user through the access service (e.g., search, display, Internet access, or a playing device), mega intermediaries may monitor the use of content by individual users on an ongoing basis.[36] Intermediaries can then collect data on users' interests, consumption habits, opinions, and tastes.[37] Online intermediaries may also enable or disable access, by either removing or blocking controversial content, or by terminating the user account altogether. "Intermediaries offer a natural point of control for monitoring, filtering, blocking and disabling" access to content,[38] which makes them ideal partners for performing civil and criminal enforcement.

The informal collaboration between government and online intermediaries is becoming an important governance tool in the twenty-first century: "In a global information network that has no geographical boundaries, law enforcement agencies are increasingly facing difficulties in gathering intelligence, finding suspects, controlling activities and generally, enforcing

---

[35] *See Top 15 Most Popular Websites*, EBIZ MBA, http://www.ebizmba.com/articles/most-popular-websites [https://perma.cc/77XM-X6DJ].

[36] Almost everything end users do on digital networks is known to private parties. Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple, and even cloud storage and synchronization services, (e.g., Dropbox), possess knowledge of what users are doing. Mobile companies know exactly where users are at almost any given time, and where they have been since joining their services. Information is the heart of most of these systems. It is essential for their operation and business models. Many of these companies analyze these stores of data for their own purposes, (e.g., marketing and research), or divulge it to other parties. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) [hereinafter Solove, *Digital Dossiers*]. For more on data mining, see for example, Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 262–70 (2008); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 353 (2008); K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 21–74 (2003).

[37] *See, e.g.*, Emilee Rader, *Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google*, TENTH SYMP. ON USABLE PRIVACY & SECURITY (SOUPS) 51, 51 (2014), https://www.usenix.org/system/files/conference/soups2014/soups14-paper-rader.pdf [https://perma.cc/H684-SPGF].

[38] *See* Niva Elkin-Koren, *After Twenty Years: Revisiting Copyright Liability of Online Intermediaries*, *in* THE EVOLUTION AND EQUILIBRIUM OF COPYRIGHT IN THE DIGITAL AGE 44 (Susy Frankel & Daniel Gervais eds., 2014).

the law."[39] As a result of this, the collaboration with online intermediaries, often global platforms, becomes essential. There are numerous examples of pressing private intermediaries into performing public functions, like enforcement, in collaboration with law enforcement agencies. Recently, in the aftermath of the 2015 Paris attacks,[40] American politicians called upon Twitter to remove pro-Islamic State Twitter accounts—the same way child-pornography sites are being tracked and blocked.[41] User accounts of the group of activists and hacktivists commonly known as Anonymous, could be considered "terrorist" as they have the potential to jeopardize national security[42]—although Anonymous has recently called upon its hackers to fight ISIS.[43] Online intermediaries are therefore called upon to decide who is a terrorist, and what should be considered a threat to public safety. Over the past decade, online intermediaries have complied with informal calls from governmental actors and society to remove content or block access to websites or users.[44]

Governments increasingly rely on informal collaboration with online intermediaries in cybersecurity, surveillance,

---

[39] Michael Birnack & Niva Elkin-Koren, *WikiHunt and the (In)visible Handshake*, OPENDEMOCRACY (Feb. 20, 2011), https://www.opendemocracy.net/michael-birnack-niva-elkin-koren/wikihunt-and-invisible-handshake [https://perma.cc/H9A7-YL2E].

[40] *See* Claire Phipps & Kevin Rawlinson, *Paris Attacks Kill More Than 120 People—As It Happened*, GUARDIAN (Nov. 14, 2015), http://www.theguardian.com/world/live/2015/nov/13/shootings-reported-in-eastern-paris-live [https://perma.cc/6G2M-UTL6].

[41] Andrew Blake, *Social Media Companies, Politicians Push to Ax Pro-ISIS Accounts*, WASH. TIMES (Dec. 7, 2015), http://www.washingtontimes.com/news/2015/dec/7/social-media-companies-politicians-push-axe-pro-is [https://perma.cc/9ZCW-MFRG]. For more on blocking child-pornography sites in the United States, see *Internet Providers Block Child Pornography*, CBS (June 23, 2008), http://www.cbsnews.com/news/internet-providers-block-child-pornography [https://perma.cc/Y9V5-C383].

[42] *See* Kevin Rawlinson & Paul Peachey, *Hackers Step Up War on Security Services*, INDEP. (Apr. 12, 2012), http://www.independent.co.uk/news/uk/crime/hackers-step-up-war-on-security-services-7640780.html [https://perma.cc/M985-GNDD].

[43] *Hacking Group Anonymous Disables Thousands of Pro-ISIS Twitter Accounts and Taking Militant Websites Offline*, DAILY MAIL (Nov. 18, 2015), http://www.dailymail.co.uk/news/article-3323597/Activist-hackers-battle-Islamic-State-cyber space.html [https://perma.cc/8W9Y-KFZM].

[44] For example, in 2010, Amazon stopped hosting WikiLeaks on its servers, and the online payment service PayPal suspended the account used by WikiLeaks to collect donations. *See* Doug Gross, *WikiLeaks Cut Off from Amazon Servers*, CNN (Dec. 2, 2010), http://www.cnn.com/2010/US/12/01/wikileaks.amazon [https://perma.cc/9MLZ-2W6H]; Robert Mendick, *Paypal Cuts Off Donations to WikiLeaks*, TELEGRAPH (Dec. 4, 2010), http://www.telegraph.co.uk/news/worldnews/wikileaks/8181140/Paypal-cuts-off-donations-to-WikiLeaks.html [https://perma.cc/SK6G-6ZA2]. Another example can be taken from 2012, in which YouTube voluntarily blocked access in Egypt and Libya to an anti-Islamic video, which ridiculed the Prophet Muhammad, titled "The Innocence of the Muslim." *See* Claire Cain Miller, *As Violence Spreads in Arab World, Google Blocks Access to Inflammatory Video*, N.Y. TIMES (Sept. 13, 2012), http://www.nytimes.com/2012/09/14/technology/google-blocks-inflammatory-video-in-egypt-and-libya.html [https://perma.cc/875T-793F].

censorship, and general law enforcement tasks.[45] Social media and search engines create gigantic archives of exchanges among identified participants, which enable surveillance at the individual and social levels.[46] The bulk of data generated by online intermediaries, combined with analytic capabilities, is often perceived as a tool that could aid law enforcement agencies in protecting the public from cybersecurity threats and terrorism.[47] Collaboration with online intermediaries could become a powerful tool in exercising law enforcement powers. Social media analytics may enable governments to find out: Who is saying what, and where is the conversation happening? What is the volume of the buzz, and what is the sentiment? Who is leading the conversation, and what is their influence? Search engines could offer governments information on search trends and individual interests. Yet, such use of governmental powers must be subject to the rule of law, or else it may severely compromise civil rights.

This form of informal collaboration was acknowledged long before Snowden's revelations. In 2003, Michal Birnhack and Niva Elkin-Koren warned against the rise of an *invisible handshake* between the government and online intermediaries. The term originates from the *invisible hand*—a metaphor coined by Adam Smith to describe the market forces that drive the economy and that often make government intervention redundant.[48] Market players, acting in their own self-interest, will react to demand, which reflects the preferences of members of society, and thus promotes the social good.[49] The *invisible handshake* is the informal coordination between the government and market players, which is executed in a legal twilight zone: while governments are authorized to operate under the rule of law within constitutional restraints, such informal PPP enables governments to bypass constitutional constraints.[50] Private

---

[45] *See generally* YOCHAI BENKLER, THE PENGUIN AND THE LEVIATHAN: HOW COOPERATION TRIUMPHS OVER SELF-INTEREST (2011).

[46] *See generally* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015).

[47] *Cf. id.* at 136 (arguing that while data mining is offered as a technique that could aid law enforcement agencies in protecting the public from cybersecurity threats and terrorism, it is "an inappropriate tool for finding terrorists").

[48] *See generally* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (Sálvio Marcelo Soares ed., 2007) (1776), http://www.ibiblio.org/ml/libri/s/SmithA_WealthNations_p.pdf [https://perma.cc/P63A-SK56].

[49] *Id.* at 349–50 ("By preferring the support of domestic to that of foreign industry, he intends only his own security; and by directing that industry in such a manner as its produce may be of the greatest value, he intends only his own gain, and he is in this, as in many other cases, led by an invisible hand to promote an end which was no part of his intention.").

[50] *See* Birnhack & Elkin-Koren, *supra* note 12, at 53–59; *see infra* Part II.

bodies are not subject to constitutional limits on search or censorship and are under no duty to respect free speech or other fundamental rights.[51] Intermediaries are often offered immunity against civil lawsuits by users whose interests were compromised by the intermediary's action or inaction.[52] By collaborating through a PPP, not only will the government avoid facing a constitutional challenge in court, market players will not be held accountable to their customers. Moreover, these players may gain the benefits of collaborating with the government, which could set government rules and regulations in their favor.[53]

All in all, both online intermediaries and governmental agents have much to gain from such informal collaboration, and are therefore likely to have strong incentives to sustain it. Yet, the exercise of governmental powers in such a legal limbo may leave citizens without an effective remedy, neither against the government nor against the mega intermediaries. Consequently, in the absence of any mechanisms for holding governments and online intermediaries accountable, informal PPPs pose a new type of threat to civil liberties.

II. A LEGAL TWILIGHT ZONE

A. Governmental Surveillance Programs: From Targeted Collection to Mass Surveillance

One response to the governance crisis created by dispersed networks is for governments to seek access to data. Governments require access to bulk data and metadata in order to analyze it for the purpose of identifying patterns and correlations, and to detect and predict potential threats to public safety, cybersecurity, and national security.[54] Governance challenges regarding access to information began prior to the emergence of the Internet. When private companies first offered telecommunications networks to the public, governments were left without legal mechanisms to control and access information. In response, governments initiated various forms of surveillance programs.

---

[51] *See* Birnhack & Elkin-Koren, *supra* note 12, at 54–55.

[52] *See infra* Section II.B.

[53] *See* Birnhack & Elkin-Koren, *supra* note 12, at 57 ("ISPs may benefit from collaborating with the government in various ways."). Jon Michaels termed these public-private partnerships as "handshake agreements." *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 904 (2008).

[54] *See generally* U.S. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014,) https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/46XK-WG5B].

U.S. government surveillance programs date back to at least the early 1930s.[55] Various forms of surveillance took place in the United States,[56] and the public was largely unaware of such programs until the Watergate scandal.[57] In 1968, Congress sought to regulate electronic surveillance for the first time.[58] The Omnibus Crime Control and Safe Streets Act conditioned the usage of electronic surveillance upon a judicial finding of *probable cause* to believe the target is committing, has committed, or is about to commit a particular enumerated offense, and that the surveillance would obtain incriminating communications about the offense.[59] However, surveillance for national security purposes was still broadly permitted.[60]

In the post-Watergate era, Congress decided to further study and regulate the proper scope of governmental operations with respect to intelligence activities.[61] In 1978, Congress implemented the recommendations of the Church Committee—a committee tasked by the U.S. Senate to study governmental operations with respect to intelligence activities—in the enactment of the Foreign Intelligence Surveillance Act (FISA).[62] FISA regulated "all electronic surveillance of American citizens or permanent residents within the United States for foreign intelligence or international counterterrorism purposes."[63] Under FISA, the Foreign Intelligence Surveillance Court (FISC) was formed, while Congress created other mechanisms for conducting surveillance outside of FISC.[64] FISC is a "secret"

---

[55] *See* S. REP. NO. 94-755, at 12 (1976) ("Since the early 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant."). For further information on U.S. surveillance prior to FISA, see G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 868–74 (2013) (describing the background of FISA enactment).

[56] For example, as part of a surveillance program named SHAMROCK, between 1947 and 1973, the U.S. government collected millions of telegrams that originated within, terminated in, or traveled through the United States. *See* S. REP. NO. 94-755, at 169.

[57] *See* Sinha, *supra* note 55, at 871–72. For more on U.S. governmental surveillance programs prior to FISA, see Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1072–94 (2006).

[58] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–803, 82 Stat. 197, 211–25 (1968) (codified at 18 U.S.C. §§ 2510–2522 (2012)).

[59] 18 U.S.C. § 2518(3) (1970); *see* Caitlin Thistle, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197, 1200–01 (2008) (summarizing the history of FISA and governmental surveillance).

[60] *See* 18 U.S.C. § 2511(3) (2012).

[61] *See* S. REP. NO. 94-755, at 12 (1976).

[62] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. § 1801 (2012)).

[63] *See* Sinha, *supra* note 55, at 873–74.

[64] In addition to FISC orders, FISA created two other forms to initiate surveillance. First, under the Attorney General's Certification to collect information related to foreign intelligence for up to one year. 50 U.S.C. § 1802 (2012). Second, when the Attorney General reasonably determines that "an emergency situation exists with respect to the

court, comprised of federal district judges who examine classified information in a closed ex-parte hearing.[65] FISC approval is generally necessary for surveillance on Americans.[66] Warrants are authorized upon a finding of "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power."[67] Thus, FISC was formed out of a need to balance the interests of the public and national security.

Beyond FISA, other forms of surveillance regulation started to emerge—perhaps most importantly, Executive Order 12,333.[68] First approved by President Ronald Reagan in 1981, "Executive Order 12333 is the principal Executive Branch authority for foreign intelligence activities *not governed by FISA*."[69] Section 2.5 authorizes the Attorney General to approve the use of any technique for intelligence purposes within the United States or against a U.S. citizen abroad:

> [F]or which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.[70]

Executive Order 12,333 is still effective, though it has been amended over the years, and it still plays an important role in U.S. surveillance programs as further noted.[71]

The biggest changes to U.S. surveillance policy, and in particular, to FISA,[72] came at the beginning of the twenty-first

---

employment of electronic surveillance to obtain foreign intelligence information." *Id.* § 1805(e). Under this second provision, the Attorney General is obliged to submit a full application in a defined timeframe from the initiation of authorization (twenty-four hours under 1978's version of FISA). *Id.* § 1805(e)(1)(D). For more on FISA, see generally Donohue, *supra* note 57.

[65] 50 U.S.C. § 1805; *see* Dia Kayyali, *What You Need to Know About the FISA Court—and How It Needs to Change*, ELEC. FRONTIER FOUND. (Aug. 15, 2014), https://www.eff.org/deeplinks/2014/08/what-you-need-know-about-fisa-court-and-how-it-needs-change [https://perma.cc/P6YL-5UKT].

[66] *See* 50 U.S.C. § 1805(a)(2)(A)–(B).

[67] *Id.* § 1805(a)(2)(A). FISC judges can grant an *ex parte* order for electronic surveillance when the application has been made by a federal officer and approved by the Attorney General, and that, on the basis of the facts, there is probable cause to believe the target is a foreign power or an agent of a foreign power and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. *See id.* § 1805(a).

[68] Exec. Order No. 12,333, 3 C.F.R. pt. 1 (1981), *amended by* Exec. Order No. 13,284, 3 C.F.R. § 18 (2004), and by Exec. Order No. 13,355, 3 C.F.R. § 2 (2005), and further amended by Exec. Order No. 13,470, 3 C.F.R. §§ 1–5 (2009).

[69] CLARKE ET AL., *supra* note 20, at 69 & n.44.

[70] Exec. Order No. 12,333, 3 C.F.R. pt. 1 (1981); EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 3 (2013), http://www.fas.org/sgp/crs/intel/R42725.pdf [https://perma.cc/3JJA-35RC].

[71] *See infra* Section II.B.

century. In the aftermath of the 9/11 attacks, the U.S. government dramatically increased surveillance efforts. First, the Bush administration ordered the NSA to eavesdrop on telephone conversations by persons in the United States to combat terrorist attacks.[73] President George W. Bush also initiated a Terrorist Surveillance Program (TSP), which operates outside of FISA, to "intercept international communications into and out of the United States" by persons linked to terrorist organizations.[74] Second, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).[75] The USA PATRIOT Act added section 215 to FISA, which allowed governmental agencies,[76] under a FISC order, to compel telecommunications providers to produce metadata[77] and

---

[72] FISA was amended in 1995 to authorize secret physical searches. 50 U.S.C. §§ 1821–1829 (2000). In 1998, Congress granted the government "pen register" and "trap-and-trace" authority by a FISA amendment, and later that year, also authorized "FISC to issue orders compelling telephone service providers to permit the government to install these devices upon a showing that the government seeks to obtain information 'relevant' to a foreign intelligence investigation." *See* 50 U.S.C. § 1842 (2012); CLARKE ET AL., *supra* note 20, at 83–84.

[73] For an overview of the legal framework of eavesdropping in the United States, see Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 17–25 (2008). These programs were presumably authorized by the President's broad and exclusive powers as Commander-in-Chief under Article II of the Constitution, "to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States," U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT OF THE UNITED STATES 6–8 (2006), https://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pdf [https://perma.cc/Y3EY-U5BZ] [hereinafter LEGAL AUTHORITIES SUPPORTING ACTIVITIES OF NSA], or alternately that Congress authorized the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001," Authorization for Use of Military Force, S.J. Res. 23, 107th Cong. § 2(a) (2001) (enacted); *see also* Adam Burton, *Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381 (2006) (discussing the legality of warrantless surveillance in the United States).

[74] LEGAL AUTHORITIES SUPPORTING ACTIVITIES OF NSA, *supra* note 73, at 5, 17; LIU, *supra* note 70, at 4–5.

[75] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). For more on the TSP, see for example, Zachery Keller, Note, *Big Brother's Little Helpers: Telecommunication Immunity and the FISA Amendment Act of 2008*, 70 OHIO ST. L.J. 1215, 1219–25 (2009).

[76] More accurately, to the director of the FBI or a designee of the director (whose rank shall be no lower than assistant special agent in charge). *See* 50 U.S.C. § 1861(a)(1) (2012).

[77] Metadata by its essence does not include the content of calls. Based on government reports, expert analysts used the acquired metadata to identify terrorist activities and "determine whether known or suspected terrorists have been in contact with" individuals in the United States. U.S. DEP'T OF JUSTICE, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2–3 (2013).

"tangible objects" if there were "reasonable grounds to believe"[78] that the tangible things sought were "relevant to an authorized investigation"[79] "into foreign intelligence, international terrorism, or espionage."[80] Congress amended this provision in 2005,[81] requiring "reasonable grounds to believe that the tangible objects sought [were] relevant to an authorized investigation (other than a threat assessment)"[82] "into foreign intelligence, international terrorism, or espionage."[83] Practically, section 215 of FISA represents a shift from the targeted collection of information to mass surveillance. Under this section, the government has employed bulk collection and "analysis of metadata associated with telephone calls within, to, or from the United States."[84]

The Protect America Act (PAA) replaced TSP in 2007.[85] It amended FISA to increase governmental agencies' ability to collect foreign communications where the collection is directed at one party that is reasonably believed to be outside the United States.[86] The PAA also granted the Attorney General and

---

[78] *See* JOHN W. ROLLINS & EDWARD C. LIU, CONG. RESEARCH SERV., R43134, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS 5 (2013). The meaning of "reasonable grounds to believe" is not defined by FISA. A report to Congress on this matter noted:

> [I]t may be helpful to look at appellate courts' interpretations of the Stored Communications Act (SCA), as it similarly authorizes law enforcement to access telecommunications transactional records (as well as stored electronic communications) upon a showing that "there are reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation." Under the SCA, the collection of stored email has been held to meet that standard in the context of a "complex, large-scale mail and wire fraud operation" in which "interviews of current and former employees of the target company suggest that electronic mail is a vital communication tool that has been used to perpetuate the fraudulent conduct" and "various sources [have verified] that [the provider who had custody of the email] provides electronic communications services to certain individual(s) [under] investigation."

Id. (second, third, and fourth alterations in original).

[79] 50 U.S.C. § 1861(b) (2012).

[80] ROLLINS & LIU, *supra* note 78, at 5. The tangible items include records, books, documents, papers, and other items. 50 U.S.C. § 1861(a) (2012). Telephony metadata can also be obtained by a national security letter (NSL). *See* 18 U.S.C. § 2709 (2012). Such a letter can be issued by the Director of the FBI or his designee, only when the "records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." *Id.* § 2709(b).

[81] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

[82] 50 U.S.C. § 1861(b)(2)(A).

[83] ROLLINS & LIU, *supra* note 78, at 4–5.

[84] U.S. DEP'T OF JUSTICE, *supra* note 77, at 2. For more on metadata, see NISO, UNDERSTANDING METADATA (2004), http://www.niso.org/publications/press/UnderstandingMetadata.pdf [https://perma.cc/3QBX-MS7D].

[85] *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552, 552–57 (2007) (formerly codified in scattered sections of 50 U.S.C.).

[86] *Id.* § 105A.

the Director of National Intelligence (DNI) the ability to authorize the acquisition of "foreign intelligence information concerning persons reasonably believed to be outside the United States . . . for periods of up to one year."[87] In that sense, the PAA excluded some intelligence activity outside of FISA.[88] Of relevance to this article, the PAA also established a framework for private sector cooperation.[89] In 2008, after the PAA expired,[90] Congress enacted the FISA Amendments Act of 2008 (FAA).[91]

The FAA expanded the types of information that intelligence agencies could obtain and added several new requirements and procedures. Most importantly, section 702 allowed the government to intercept Internet and telephone content of non-citizens abroad without individualized court orders.[92] With some limitations,[93] the Attorney General and the DNI could jointly authorize the targeting of non-U.S. persons reasonably believed to be located outside the United States for periods of up to one year.[94] The FAA added a new requirement that, when targeting U.S. citizens abroad, the government must obtain an individualized court order (removing the power granted to the Attorney General and the DNI by the PAA).[95] Congress also expanded the pre-warrant surveillance window for "emergencies" from seventy-two hours to one week.[96]

The metadata program took a turn in 2015. On May 7, the U.S. Court of Appeals for the Second Circuit ruled that the

---

[87] *Id.* § 105B. For more on the PAA, see Juan P. Valdivieso, Recent Developments, *Protect America Act of 2007*, 45 HARV. J. ON LEGIS. 581 (2008).

[88] Valdivieso, *supra* note 87, at 582 (analyzing the PAA provisions).

[89] *Id.* at 584 (analyzing PAA's Private Sector provisions). Under authorized acquisition, the Attorney General and the DNI can issue a directive to an individual to "provide the government with all information, facilities, and assistance necessary to accomplish the acquisition[,] . . . [and] compensate [them for their participation] at the prevailing rate." Protect America Act of 2007 § 105B(e), (f). ELIZABETH B. BAZAN, CONG. RESEARCH SERV., RL34143, P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 8–9 (2008), http://www.fas.org/sgp/crs/intel/RL34143.pdf [https://perma.cc/8BTE-YFNQ].

[90] The Protect America Act had a time limit of six months for new Directives to be issued. *See* Protect America Act of 2007 § 6.

[91] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008). For more on the FAA, *see* Keller, *supra* note 75, at 1226–35.

[92] *See* 50 U.S.C. § 1881a(a).

[93] The government may not: (1) "intentionally target any person known at the time of acquisition to be located in the United States;" (2) "intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;" (3) "intentionally target a United States person reasonably believed to be located outside the United States;" (4) "intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;" and (5) must be "consistent with the fourth amendment." *Id.* § 1881a(b).

[94] *Id.* § 1881a(a).

[95] *Id.* § 1881c(a)(2).

[96] *Id.* § 1805(e).

bulk metadata program exceeded the authorization granted by section 215 of the PATRIOT Act, as requests must be tailored to fit a particular investigation.[97] Shortly after, on June 1, section 215 expired. One day later, Congress enacted the USA Freedom Act,[98] which prohibited any bulk collection of Americans' calling records by the NSA.[99] The Act initiated a new telephone metadata program in which companies would store metadata and NSA analysts could query the information under prescribed legal conditions.[100] This new program added more transparency to the secret FISA court. The National Security Agency Civil Liberties and Privacy Office was obliged to submit a transparency report on the implementation of the Act, which they released for the first time on January 15, 2016.[101]

Ultimately, the need to secure government access to information that resides on private facilities invoked a legal response. Both the executive branch and the legislature responded by implementing various forms of regulation under the rule of law. Yet, the growing need to ensure ongoing access to bulk data held by online intermediaries required some level of participation by the online intermediaries that control this data. To address this challenge, governance by proxy emerged.

B. The New Form of Governance Through Public Private Partnerships

In 2013, Edward Snowden verified the existence of an informal collaboration between the government and online intermediaries—the *invisible handshake*.[102] The Snowden revelations made the new type of PPP visible, at least to some extent. The public learned that the private sector transferred various forms of information to governmental agents.[103] Based on information that was made available, the public learned that the NSA collected cyber intelligence[104] (metadata and electronic

---

[97] *See* ACLU v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015).

[98] *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

[99] *Id.* § 201. For an analysis of the USA FREEDOM Act, see Bart Forsyth, *Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection*, 72 WASH. & LEE L. REV. 1307, 1321–40 (2015); Erin Kelly, *Senate Approves USA FREEDOM Act*, USA TODAY (June 2, 2015), http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747 [https://perma.cc/689P-LYV8].

[100] *See* USA FREEDOM Act of 2015 §§ 101, 103.

[101] *See* Aisha Chowdhry, *What's Missing in the New NSA Report?*, FCW (Jan. 15, 2016), https://fcw.com/articles/2016/01/15/nsa-privacy-chowdhry.aspx [https://perma.cc/2X3G-WVGE].

[102] *See infra* note 105.

[103] *See* Solove, *Digital Dossiers*, *supra* note 36, at 1084 (arguing that information flows from private companies to the government).

[104] *See generally* ROLLINS & LIU, *supra* note 78.

communications*)* via online intermediaries through two sub-programs: PRISM and upstream collection.[105] The NSA also conducted other external programs that usually depended on global partnerships with other intelligence agencies and perhaps with other forms of surveillance.[106] In some instances, law enforcement officials installed devices at online intermediaries' hosting facilities to locate information (e.g., e-mail traffic).[107] Additionally, several private sector entities had contracts with the government, allowing the government to acquire databases of personal information.[108] Snowden's leaked documents suggested that nine Internet companies were specifically involved in a

---

[105] Data received from all of NSA programs is stored and remains searchable by NSA agents using various software, e.g., XKeyscore. *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet*,' GUARDIAN (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [https://perma.cc/363C-KE6G]. According to Snowden, XKeyscore grants NSA analysts the ability to search through an entire database of information, even "real-time" interception of an individual's Internet activity, which was obtained through various methods. *Id.* As Snowden claimed in his first video interview after his revelations: "'I, sitting at my desk' . . . could 'wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email.'" *See* Laura Poitras & Glenn Greenwald, *NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society that Does These Sort of Things'—Video*, GUARDIAN (June 9, 2013), http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video [https://perma.cc/WHT4-79MQ]. Thus, under this revelation, the NSA obtained information without court orders, outside of FISA, although the NSA is required to obtain an individualized warrant for the targeting of U.S. persons. Greenwald, *supra.* Snowden's revelations show that the NSA intercepts the communications of U.S. persons without a warrant or court order. *See id.*

[106] Intelligence agencies may have gathered information obtained by Smartphone applications. As reported by the Guardian, the NSA and its UK counterpart GCHQ took advantage of "leaky" smartphone applications such as the Angry Birds game made by Rovio Entertainment Ltd. James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, GUARDIAN (Jan. 28, 2014), http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [https://perma.cc/Q6JR-RNTR]. However, the leaked documents did not disclose the method with which the intelligence agencies are obtaining this information, nor how many users may be affected. *Id.* Saara Bergström, Rovio's VP of marketing and communications, denied knowledge of such programs: "Rovio doesn't have any previous knowledge of this matter, and h[as] not been aware of such activity in 3rd party advertising networks . . . . Nor do we have any involvement with the organizations you mentioned." *Id.* Hence, it is difficult to assess the public-private partnership in this matter.

[107] *See generally* E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH. 10 (2001) (summarizing the FBI's Carnivore project which enables agents to utilize technology to intercept, filter, seize, and decipher digital communications on the Internet); Solove, *Digital Dossiers*, *supra* note 36, at 1098–99 (summarizing the various methods in which the government uses information obtained by online intermediaries).

[108] *See* Solove, *Digital Dossiers*, *supra* note 36, at 1095–96 (giving ChoicePoint as an example of a private sector company that has contracts with federal agencies) (citing Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1).

surveillance program termed PRISM: Microsoft, Yahoo!, Google, Facebook, Paltalk, AOL, Skype, YouTube, and Apple.[109]

The revealed NSA practices demonstrate how PPPs, despite their benefits, could endanger the rule of law and civil liberties, mainly due to the legal twilight zone in which they operate. The fact that the existence of PPPs is no longer secret might affect the nature of the PPP relationship. It could generate consumer pressure on online intermediaries to abandon such practices.[110] Yet the invisible handshake was not only simply "invisible" in the sense that it was kept secret; it was also "invisible" to the law. Online intermediaries, as profit-maximizing market players, are generally free to run their privately owned facilitates and voluntarily share information at their discretion, subject to regulatory restrictions and contractual obligations to their users.[111] Similarly, PPPs may also escape constitutional restraints so long as no governmental powers are exercised.

PPPs in the United States—in terms of voluntary disclosure of information—are not entirely new. They existed at least as early as the 1970s with the formation of the NSA's Special Source Operations (SSO) division.[112] At that time, over one hundred trusted U.S. companies cooperated with the SSO.[113] Long before the 9/11 attacks, and more importantly, outside the scope of FISA or a Presidential order, the NSA sought partnerships with private companies.[114] According to the *New York Times*, nearly seven months before the 9/11 attacks, the NSA asked Qwest Communications for customers' call records,

---

[109] *See* Greenwald & MacAskill, *supra* note 8. For skepticism on the involvement of the nine companies in PRISM, see Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date [https://perma.cc/UKS9-SVBA] ("It's hard to be sure, but the number of companies that have issued denials, and the vehemence of some of their statements, suggests that they may be sincere.").

[110] For a discussion on how market forces failed to reshape the nature of such PPP, see *infra* Section IV.A.

[111] *See infra* Part III.

[112] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/G9DS-NKSD].

[113] *Id.*

[114] Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES (Oct. 14, 2007), http://www.nytimes.com/2007/10/14/business/14qwest.html?ref=%20todayspaper&_r=0 [https://perma.cc/3HFJ-GD96].

without a warrant.[115] Similar accusations were made regarding AT&T as part of a court filing.[116]

Generally, the 9/11 attacks changed the nature of the invisible handshake. Although some companies collaborated with the government prior to the 9/11 attacks, other companies refused to furnish information without a warrant.[117] After 9/11, due both to patriotism and the new legal regime, which granted immunity for voluntary collaboration, more private companies collaborated with the government.[118]

The incentives for the government to form such PPPs are obvious; data held by online intermediaries could extend well beyond any intelligence information gathering. For one thing, individuals are more likely to provide personal information to a private entity.[119] Although the government already collects massive amounts of data directly from individuals,[120] such information sharing with the private sector is more frequent and broad.[121] Furthermore, private companies face fewer restrictions on data mining.[122] Thus, it is not surprising that the NSA wishes to obtain such information, indeed, the NSA can obtain similar data by seeking a warrant. Yet voluntary disclosure of information could not only make it easier for the NSA to obtain the data, but may also enable access to larger amounts of information,[123] even in "real time."

There are two known types of voluntary disclosure of information between the government and private companies. One type of disclosure involves the active participation of

---

[115] *Id.*

[116] Andrew Harris, *Spy Agency Sought U.S. Call Records Before 9/11, Lawyers Say*, 911TRUTH.ORG (July 12, 2006), http://www.911truth.org/spy-agency-sought-u-s-call-records-before-911-lawyers-say/ [https://perma.cc/4HC7-RF5Z].

[117] For such examples, see Solove, *Digital Dossiers*, *supra* note 36, at 1097 (listing bookstore's records and Amazon.com information which were not disclosed to governmental agencies).

[118] *Id.* at 1096–97.

[119] Michaels, *supra* note 53, at 908 ("People simply do not interface with the government in the same ways or with the same frequency as they do with the private sector, and thus the intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources.").

[120] For more on the wide variety of methods the U.S. government uses to obtain personal information directly, see Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. CIV. RTS.-CIV. LIBERTIES. L. REV. 435, 439–51 (2008).

[121] *See* Michaels, *supra* note 53, at 908.

[122] *Id.* ("[P]rivate data gathering is subject to less stringent regulation than what the government faces.").

[123] Voluntary programs to aid the government in detecting and preventing terrorist attacks extend far beyond the traditional PPP. For example, in the wake of 9/11, the Justice Department developed a nationwide program "giving millions of American truckers, letter carriers, train conductors, ship captains, utility employees, and others a formal way to report suspicious terrorist activity." Jon D. Michaels, *Deputizing Homeland Security*, 88 TEX. L. REV 1435, 1444–46 (2010).

private companies, which grants the government access to information and metadata beyond the legal requirements. Put simply, Internet companies hand out information without any legal obligation to do so.[124] The other type of voluntary disclosure occurs when online intermediaries enable interception of their systems, intentionally introduce backdoors into their systems, or allow the government to directly tap into their services.[125] The public became aware of the following two methods of disclosure due to Snowden's revelations.

The first method of voluntary disclosure of data was conducted under a program code-named PRISM (a computer system) through which the NSA allegedly collected data directly from the central servers of nine U.S. Internet companies. The NSA allegedly extracted audio and video chats, photographs, e-mails, documents, and connection logs of non-U.S. persons outside the United States.[126] Presumably, companies granted the NSA access to their servers, and effectively handed over information.[127] PRISM was arguably governed by section 702 of FISA.[128]

In the second method, designed to fill gaps in the information collected under PRISM,[129] the NSA used upstream collection,[130] which is the gathering of electronic communications on fiber networks and infrastructure (the Internet backbone).[131]

---

[124] *See infra* notes 126–128.

[125] "[B]ackdoor[s] [are] . . . intentional flaw[s] in a cryptographic algorithm or implementation, . . . allow[ing] . . . bypass[ing] of security mechanisms." Nick Sullivan, *How the NSA (May Have) Put a Backdoor in RSA's Cryptography: A Technical Primer*, ARSTECHNICA (Jan. 5, 2014), http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer [https://perma.cc/3PE4-A6QR]. It is like a secret tunnel in an almost unbreakable wall. *Id.*

[126] *See* Gellman & Poitras, *supra* note 112; Greenwald & MacAskill, *supra* note 8.

[127] In addition to Snowden's revelation on PRISM, USA Today reported that the major U.S. telecommunications companies (AT&T, Verizon, and BellSouth) turned over their "call-detail records" (metadata) to the NSA since 9/11, in a secret deal. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (Nov. 5, 2006), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm [https://perma.cc/XE4A-8SLP]; Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY (June 30, 2006), http://www.usatoday.com/news/washington/2006-06-30-nsa_x.htm [https://perma.cc/A6M9-2A7U]. However, after BellSouth and Verizon denied their involvement, and demanded that newspaper to retract the report, USA Today withdrew the story as it applied to them. Stephen Manuel Wolfson, Note, *The NSA, AT&T, and the Secrets of Room 641A*, 3 I/S: J.L. & POL'Y INFO. SOC'Y 411, 413 (2007–2008) (describing USA Today's news articles).

[128] *See* 50 U.S.C. § 1881a (2012); ROLLINS & LIU, *supra* note 78, at 3.

[129] As later revealed, the vast majority of communications obtained under section 702 are from online intermediaries and not upstream collection. ROLLINS & LIU, *supra* note 78, at 4; *see generally* Memorandum Opinion at *9, 2011 WL 10945618 (FISA Ct. Oct. 3, 2011).

[130] Upstream collection is defined as "acquisition while Internet traffic is in transit from one unspecified location to another." ROLLINS & LIU, *supra* note 78, at 4.

[131] *See NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents [https://perma.cc/X58K-FYSX].

The information collected under this method included the metadata and content of foreign targets overseas whose communications flowed through American networks. Upstream collection was first revealed back in 2006, during an Electronic Frontier Foundation (EFF) class action lawsuit against AT&T.[132] In his statement, Mark Klein, a former AT&T technician, reported that AT&T used a "splitter" device to make a complete copy of the Internet traffic that AT&T received, and then divert it onto a separate fiber-optic cable connected to a room controlled by the NSA.[133] At that same time, lawsuits were filed against other telecommunications companies on similar grounds.[134] Eventually, the telecommunications companies and the government were awarded retroactive immunity from liability under the FAA,[135] and the cases were dismissed.[136] The FAA made it clear: until 2008, there was a warrantless partnership between major U.S. telecommunications companies and the NSA. Currently, upstream collection is arguably legal under section 702 of FISA and Executive Order 12,333.[137]

The new challenges to governance also take the form of global partnerships. Along with the two known "internal" programs, the NSA also cooperates with other intelligence agencies overseas, and conducts various surveillance programs. One example of such program is MUSCULAR—a surveillance project operated by the NSA and the British Government Communications Headquarters (GCHQ). This project operates in Britain and exploits data gathered from links between Yahoo!'s and Google's data centers, "including both metadata

---

[132] Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978 (N.D. Cal. 2006).

[133] *See Wiretap Whistle-Blower's Account*, WIRED (Apr. 7, 2006), http:// archive. wired.com/science/discoveries/news/2006/04/70621 [https://perma.cc/TL78-XXD2]; *AT&T's Role in Dragnet Surveillance of Millions of Its Customers*, ELEC. FRONTIER FOUND., https://www.eff.org/files/filenode/att/presskit/ATT_onepager.pdf [https://perma.cc/G7CK-Y42W]. The report was complemented by an expert opinion by J. Scott Marcus. *See* Declaration of J. Scott Marcus in Support of Plaintiffs' Motion for Preliminary Injunction, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-0672-VRW).

[134] These lawsuits "were combined into a multi-district litigation proceeding named In re NSA." *See Hepting v. AT&T*, ELEC. FRONTIER FOUND., https://www.eff.org/ cases/hepting [https://perma.cc/662U-4682].

[135] In 2008, Congress added section 702 to FISA, and thereby created immunity for telecommunications companies that aided the government during the period beginning on September 11, 2001, and ending on January 17, 2007. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 201, 122 Stat. 2436, 2468–70 (2008) (codified at 50 U.S.C. § 1885(a) (2012)) (adding § 802 to FISA). Under this section, the Attorney General can file a certification in a lawsuit for such immunity, and the court can dismiss the case against the telecommunications company. *See* 50 U.S.C. § 1885a (2012).

[136] *See supra* note 134.

[137] *See* 50 U.S.C. § 1881a; Exec. Order No. 12,333, 3 C.F.R. pt. 1 (1981); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2140–42 (2014).

and content like audio, video[,] and text."[138] On the American side, this program runs under Executive Order 12,333.[139]

Briefly after Snowden's revelations, the companies linked to PRISM, upstream collection, and global data collection partnerships denied their involvement, suggesting that they would only turn over information in the face of legitimate, specific requests to do so.[140] The Final Report of the Review

---

[138] *See* Mark Jaycox, *Three Leaks, Three Weeks, and What We've Learned About the US Government's Other Spying Authority: Executive Order 12333*, ELEC. FRONTIER FOUND. (Nov. 5, 2013), https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying [https://perma.cc/5U7S-ZSSQ]; Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [https://perma.cc/22PT-RC38].

[139] *See* Jaycox, *supra* note 138.

[140] Specifically, Google announced:

> We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a 'back door' for the government to access private user data.

Dominic Rushe & James Ball, *PRISM Scandal: Tech Giants Flatly Deny Allowing NSA Direct Access to Servers*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining [https://perma.cc/KP6F-R8H5]. "An Apple spokesman said: 'We have never heard of PRISM. We do not provide any government agency with direct access to our servers and any agency requesting customer data must get a court order.'" *Id.* Facebook's chief security officer, Joe Sullivan "said it did not provide government organisation with direct access to Facebook servers. 'When Facebook is asked for data or information about specific individuals, we carefully scrutinise any such request for compliance with all applicable laws, and provide information only to the extent required by law.'" *Id.* Microsoft said:

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

Id. A Yahoo! spokesman said: "Yahoo! takes users' privacy very seriously . . . . We do not provide the government with direct access to our servers, systems, or network." Gellman & Poitras, *supra* note 112. Other media reports insisted that the Guardian and Washington Post reports were "incorrect and appear to be based on a misreading of a leaked PowerPoint document." Declan McCullagh, *No Evidence of NSA's 'Direct Access' to Tech Companies*, CNET (June 7, 2013), http://www.cnet.com/news/no-evidence-of-nsas-direct-access-to-tech-companies [https://perma.cc/K8D3-DUF9]. Hence, under this argument, the NSA "has not obtained direct access to the systems of Apple, Google, Facebook, and other major Internet companies." *Id.* However, NSA's General Counsel Rajesh De admitted that the companies knew about the NSA's collection of data under both PRISM and some unnamed "upstream" collections on the communications links. *See* Spencer Ackerman, *US Tech Giants Knew of NSA Data Collection, Agency's Top Lawyer Insists*, GUARDIAN (Mar. 19, 2014), http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de [https://perma.cc/2FBZ-22JF]; *see also* Greenwald & MacAskill, *supra* note 8; Rushe & Ball, *supra* note 140; Bruce Schneier, *Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong*, THE ATL. (Mar. 25, 2014), http://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-

Group on Intelligence and Communications Technologies—a review group formed by the DNI following Snowden's revelations—argued that, after reviewing the allegations that the government had intentionally introduced "backdoors" into commercially available software, they were "unaware of any vulnerability created by the US Government in generally available commercial software that put[s] users at risk of criminal hackers or foreign governments decrypting their data."[141] Moreover, they concluded that "in the vast majority of generally used, commercially available encryption software, there [was] no vulnerability, or 'backdoor,' that ma[de] it possible for the US Government or anyone else to achieve unauthorized access."[142]

Due to the secrecy of the alleged PPP that Snowden revealed—and because there was no admission of such PPP by any of the nine Internet companies—it could not be completely certain whether and to what extent companies voluntarily shared information with the government under PRISM. What is evident, however, is that many U.S. service providers did not encrypt parts of their services, which allowed, intentionally or not, government agencies to collect this data rather easily.[143] Yahoo!, for example, did not encrypt their Internet users' connections by default, which allowed the NSA to collect e-mail address books and "buddy" lists.[144] Only after the PRISM revelations, on the same day to be exact, Yahoo! announced that they would enable SSL encryption by default for users logging into its web-based mail service.[145] A few months after Snowden's

---

strong/284612 [https://perma.cc/U75P-HHMZ]; *Google Statement on NSA Infiltration of Links Between Data Centers*, WASH. POST (Oct. 31, 2013), http://www.washingtonpost.com/world/national-security/google-statement-on-nsa-infiltration-of-links-between-data-centers/2013/10/30/75f3314a-41b3-11e3-a624-41d661b0bb78_story.html [https://perma.cc/QQ7F-SA9C].

141 *See* CLARKE ET AL., *supra* note 20, at 217.

142 *Id.*

143 *See* Bruce Schneier, *A Fraying of the Public/Private Surveillance Partnership*, THE ATL. (Nov. 8 2013), http://www.theatlantic.com/technology/archive/2013/11/a-fraying-of-the-public-private-surveillance-partnership/281289 [https://perma.cc/D5W5-2YYU].

144 The Yahoo! buddy list contains the names and contact information for all of the user's friends which were contacted using the Yahoo! service. *See* Shannon Cotton, *How to View My Yahoo! Instant Messenger Buddy List*, TECHWALLA, https://www.techwalla.com/articles/how-to-view-my-yahoo-instant-messenger-buddy-list [https://perma.cc/H87B-VBRP].

145 Andrea Peterson et al., *Yahoo to Make SSL Encryption the Default for Webmail Users. Finally.*, WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/14/yahoo-to-make-ssl-encryption-the-default-for-webmail-users-finally [https://perma.cc/3QFR-QHNW].

revelations, Google announced that its mail service, Gmail, would (now) be more secure from government spying.[146]

Primarily in light of Snowden's revelations, both the executive branch and Congress sought to officially legalize and encourage PPPs. In February 2015, President Barack Obama signed an executive order that "urge[d] companies to share *cybersecurity-threat information*" with the federal government and with other companies.[147] The Executive Order, "advisory in nature, . . . encourage[d] the development of central clearinghouses for companies and the government to share data."[148] Moreover, it encouraged the creation of data sharing centers across specific geographic regions.[149]

In mid-December 2015, President Obama signed the Omnibus Appropriations Act, which included a provision titled the Cybersecurity Act of 2015.[150] The first chapter of the Cybersecurity Act is a rendition of a highly controversial bill called the Cyber Information Sharing Act (CISA).[151] For cybersecurity purposes, the Cybersecurity Act authorizes private entities to monitor their information systems, operate defensive measures, and share "cyber threat indicators" or "defensive measures" for a cybersecurity purpose.[152] Essentially, the Act regulates information sharing between private entities and the government on vague and loose terms.

The importance of the Cybersecurity Act, and the new Executive Order on PPPs, is vast. It is not surprising that these actions occurred after Snowden's revelations. When the handshake was "invisible," there was no need for such acts

---

[146] *See* Chris Welch, *Google Encrypts Gmail Between Data Centers to Keep the NSA Out of Your Inbox*, THE VERGE (Mar. 20, 2014), http:// www. theverge. com/2014/3/20/5530072/google-encrypts-gmail-between-data-centers-to-keep-out-nsa [https:// perma. cc/K3CT-VXLE].

[147] Katie Zezima, *Obama Signs Executive Order on Sharing Cybersecurity Threat Information*, WASH. POST (Feb. 12, 2015), http://www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity threats/?tid=sm_tw [https://perma.cc/45ET-YPJQ] (emphasis added).

[148] *Id.*

[149] *Id.*

[150] *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2016).

[151] *See* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015) (enacted). For criticism on previous versions of CISA, see for example, Sam Thielman, *Controversial Cybersecurity Bill on Hold as Experts Charge It Won't Stop Hackers*, GUARDIAN (Aug. 5, 2015), http://www.theguardian.com/world/2015/aug/05/cybersecurity-cisa-bill-hackers-privacy-surveillance [https://perma.cc/R9AU-2LMV]; Eldar Haber, *The Cybersecurity Information Sharing Act (CISA)*, CYBER BLOG (Aug. 7, 2015, 7:27 PM), http://weblaw.haifa.ac.il/he/Research/ResearchCenters/cyberforum/cyberblog/Lists/Posts/Post.aspx?ID=20 [https://perma.cc/MX4Y-5M2Q].

[152] *See* Consolidated Appropriations Act of 2016 § 104.

because most companies cooperated with the government.[153] As these companies now feared alienating their costumers, they sought some form of transparency. Some companies, like Apple, began to publicly oppose aiding governmental agencies even after receiving a court order.[154] The state further attempted to aid those companies in reducing the probability of alienating their customers through public statements made by the President during a press conference that explained the importance of PPPs,[155] while emphasizing the crucial role of the industry in national security protection. The now-visible PPPs seek approval from citizens in order to eliminate any potential barriers to private sector cooperation, which were caused mainly by Snowden's revelations.

As this part shows, over the past two decades, governments have adjusted their strategies for governing the digital environment, using online intermediaries in innovative ways. Yet, the social institutions that sought to secure the rule of law and civil liberties fell short of addressing this informal PPP. Part III addresses these legal gaps.

III. SECURING CIVIL LIBERTIES IN THE INVISIBLE HANDSHAKE

Whether FISA or the Executive Order are constitutional is debatable,[156] and beyond the scope of this article.[157] This part

---

[153] *See infra* note 233.

[154] *See infra* note 248. However, it should be noted that Apple, while allegedly involved in PRISM, does not necessarily represent every online intermediary as their business model relies less on information, and therefore their concern in this matter relies on protecting their products and keeping their customers. For more information on Apple's current business model, see Jitender Miglani, *How Apple Makes Money? Understanding Apple Business Strategy*, R&P (Jan. 1, 2016), http://revenuesandprofits.com/how-apple-makes-money [https://perma.cc/Z6RW-WUC7].

[155] "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners." *See* Zezima, *supra* note 147 (quoting President Obama's speech at the first White House Summit on Cybersecurity and Consumer Protection held at Stanford University).

[156] Any Act, e.g., FISA, must be held to not violate constitutional rights for its validity. Executive Order 12,333 restricts intelligence collection not consistent with the Constitution. *See generally* Exec. Order No. 12,333, 3 C.F.R. pt. 2.1 (1981).

[157] Many scholars criticized FISA as unconstitutional or the NSA programs as violating the statutory language of FISA. *See, e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014); Patrick Walsh, *Stepping On (or Over) the Constitution's Line: Evaluating FISA Section 702 in a World of Changing "Reasonableness" Under the Fourth Amendment*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 741 (2015); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J.L. & PUB. POL'Y 901 (2014). In addition, the Supreme Court ruled that wide-sweeping surveillance could also result in a violation of the Fourteenth Amendment's Equal Protection Clause, as it could involve monitoring individuals on the basis of their race or ethnicity. For this argument, see

focuses on how the informal partnership between government and online intermediaries affects civil liberties. Civil liberties are generally secured by constitutional safeguards, yet private companies are not subject to constitutional barriers.[158] If governments can easily bypass constitutional restraints by co-opting the private sector, are civil liberties sufficiently secured? This legal inquiry is further divided into the constitutional aspects of the invisible handshake and the statutory framework within which it operates.

A. Constitutional Aspects

The Constitution generally protects individuals from the state.[159] This "state-citizen" dimension can be characterized as the governmental paradigm.[160] The invisible handshake, however, presents a more complex relationship: state-online intermediaries, and, online intermediaries-citizen.[161] The Constitution may apply to the state-online intermediaries' relationship,[162] however, the Constitution does not generally play a role in the online intermediaries-citizen relationship, unless online intermediaries are deemed state actors. Otherwise, citizens' relationships with online intermediaries are governed by private law.[163] Does the voluntary nature of the invisible handshake mandate treating online intermediaries as state actors that are governed by the Constitution? And if so, which constitutional concerns would be triggered?

The invisible handshake clearly raises a series of constitutional concerns.[164] When the government acquires

---

Cindy C. Unegbu, Comment, *National Security Surveillance on the Basis of Race, Ethnicity, and Religion: A Constitutional Misstep*, 57 HOW. L.J. 433 (2013). Until now, one federal court has held that one of the NSA programs violated the Fourth Amendment. *See* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013). Other courts held that section 702 does not violate the Fourth Amendment. *See, e.g.*, Hasbajrami v. United States, Nos. 13-CV-685, 11-CR-623, 2014 WL 4954596 (E.D.N.Y. Oct. 2, 2014); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or. June 24, 2014); United States v. Muhtorov, No. 1:12-cr-00033-JLK, 2013 U.S. Dist. LEXIS 61756 (D. Colo. Apr. 30, 2013).

158 *See* Birnhack & Elkin-Koren, *supra* note 12, at 49–50.

159 *Id.* at 48–49.

160 *Id.* at 49–50 (coining the term "Governmental Paradigm").

161 *Id.*

162 *Id.*

163 *See id.* at 51–53.

164 Beyond the reasons listed in this part, there is another potential claim solely against the NSA. The NSA's actions could be in violation of the Administrative Procedures Act (APA). *See* 5 U.S.C. § 701(b)(1) (2012). Under the APA, any person who suffered a "legal wrong" due to agency action, or was adversely affected or aggrieved by such action, shall be entitled to judicial review. *Id.* § 702. This provision requires an "agency action," defined as "the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." *Id.* § 551(13). As NSA actions seem more like a generalized

personal information via informal channels, without judicial review, it may potentially violate the fundamental principles of separation of powers.[165] Treating online intermediaries as state actors triggers two main constitutional claims by citizens: violations of their First and Fourth Amendment rights.[166]

The First Amendment protects against governmental infringement of the freedom of speech and the freedom of association (the right to belong to any lawful political party or association).[167] A government actor's actions could violate these rights—in this context, mainly the freedom to associate.[168] Possible chilling effects on the freedom to associate could occur under PPPs, as individuals will fear associating and expressing political views as a member of a group. Individuals might fear that their online activities are viewed and stored by government agents, and therefore they might minimize their engagement or cease their online activities altogether. Thus far, courts have declined to apply the First Amendment to similar cases involving state actors.[169]

---

practice, voluntary disclosure of information by a third party will most likely fall out of this category. *See* ACLU v. NSA, 493 F.3d 644, 678–79 (6th Cir. 2007) (discussing the "agency action" definition when relating to NSA alleged conduct).

[165] Warrantless wiretapping may elicit a constitutional challenge under the Separation of Powers Doctrine. Accordingly, when a governmental agent, e.g., the NSA, conducts warrantless wiretapping, its action is contrary to the limits imposed by Congress. For further information on the Separation of Powers Doctrine, see for example, INS v. Chadha, 462 U.S. 919 (1983); Buckley v. Valeo, 424 U.S. 1 (1976); Keller, *supra* note 75, at 1239–41 (examining whether the FAA violates the Separation of Powers Doctrine). For a similar argument, see *ACLU*, 493 F.3d at 674.

[166] Arguably, the invisible handshake may also implicate the Fifth Amendment as the individual's property (which information was obtained) could be deemed as deprived without due process of law. *See* U.S. CONST. amend. V. In this case, Americans are unaware of the invisible handshake, and are therefore deprived of judicial process through which they could seek redress.

[167] U.S. CONST. amend. I. For more on free association rights in light of NSA surveillance practices, see Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008) (arguing "that the First Amendment's freedom of association guarantees . . . provide a proper framework for regulating relational surveillance").

[168] FISA has been challenged on First Amendment grounds a few times since its enactment. *See ACLU*, 493 F.3d at 696; ACLU v. NSA, 438 F. Supp. 2d 754, 758, 767–68 (E.D. Mich. 2006); United States v. Falvey, 540 F. Supp. 1306, 1314–15 (E.D.N.Y. 1982). For a recent case on the potential violation of the freedom to associate by NSA programs, see First Amended Complaint for Constitutional and Statutory Violations Seeking Declaratory and Injunctive Relief, First Unitarian Church of L.A. v. NSA, No. 3:13-cv-03287 JSW (N.D. Cal. Sept. 9, 2013). For more on NSA programs and the First Amendment, see generally Thistle, *supra* note 59. For more on freedom to associate, see NAACP v. Alabama, 357 U.S. 449, 460 (1958) (finding a First Amendment violation for turning over membership lists).

[169] *See* ACLU v. Clapper, 785 F.3d 787, 821 n.12 (2d Cir. 2015) (declining to discuss the Plaintiff-Appellant's First Amendment claims); *ACLU*, 493 F.3d at 657 ("On a straightforward reading, this claim does not implicate the First Amendment."); Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983) (noting that

The Fourth Amendment grants people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and ensures that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[170] The Fourth Amendment can be violated only if a "search" is conducted. Thus, the question is whether government actors' actions constitute a "search" under this provision.[171]

To meet the Fourth Amendment's "search" standard a person invoking its protection must be able to claim a "legitimate expectation of privacy" that has been invaded by government action.[172] Two questions are usually embraced under this inquiry: (1) whether the individual has exhibited an actual expectation of privacy; and (2) whether that expectation is one that society is prepared to recognize as "reasonable."[173] In the informal PPP context, the question is whether data collected through online intermediaries collaborating with the government constitutes an unreasonable search. The *third-party doctrine*, however, posits that there is no "legitimate expectation of privacy" under the Fourth Amendment in the contents that individuals disclose in commercial transactions because one

---

surveillance that falls under the Fourth Amendment "does not violate First Amendment rights, even though it may be directed at communicative or associative activities").

[170] U.S. CONST. amend. IV.

[171] Blake Covington Norvell, *The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation?*, 11 YALE J.L. & TECH. 228, 233 (2009) ("In approaching a question of whether the Fourth Amendment has been violated, one must first determine if a 'search,' conducted by or on behalf of the government, has taken place.").

[172] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[173] *Id.* Prior to *Katz*, the Supreme Court ruled in 1928 that the Fourth Amendment did not apply to telephone conversations. *See* Olmstead v. United States, 277 U.S. 438 (1928). In 1979, the Supreme Court held that the installation and use of a "pen register," 18 U.S.C. § 3127(3) (2012), was not a search within the meaning of the Fourth Amendment, and hence no warrant was required. Smith v. Maryland, 442 U.S. 735, 746–47 (1979). The telephone numbers that a customer dialed were not protected by the Fourth Amendment as they were disclosed to the telephone company. *Id.* at 745. In *United States v. Knotts*, the Supreme Court continued *Katz*'s ruling, holding that a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. United States v. Knotts, 460 U.S. 276, 286 (1983). In 2010, the Supreme Court held that reading text messages sent and received on a pager the employer owned and issued to an employee could constitute a "search" but it was reasonable and did not violate respondents' Fourth Amendment rights. City of Ontario v. Quon, 560 U.S. 746 (2010); *see* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 583–84 (2011) (describing the history prior to *Katz v. United States*). However, despite the Supreme Court ruling in *Olmstead* and prior to *Katz*, Congress made wiretapping a federal crime shortly thereafter. *See* Federal Communications Act of 1934, Pub. L. No. 90-351, § 2520, 48 Stat. 1103 (codified at 47 U.S.C. § 605 (2012)); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 492 (2006) (describing the history of privacy in wiretapping).

has "assumed the risk" that this information might at some point be disclosed.[174] In other words, under this doctrine, there is no Fourth Amendment expectation of privacy in information conveyed from users to intermediaries.[175]

The Supreme Court recently reinvigorated the third-party doctrine. In *United States v. Jones*,[176] the Court held that a month-long Global Positioning System (GPS) tracking of a vehicle was a trespassory intrusion upon private property that constituted a Fourth Amendment search, mainly due to the physical intrusion caused by attaching the GPS to the vehicle.[177] How applicable is *Jones* to the invisible handshake? In *Jones*, when the government installed a device on the vehicle, it "physically occupied private property."[178] Would the Court have reached the same outcome if the government had obtained information from a GPS that was already installed in the vehicle and used by Jones? The Court noted that it might reach a similar outcome if such a case presented itself.[179] While no certainty lies here, this ruling is arguably less applicable to the invisible handshake. *Jones* did, however, provide some insights to the new challenges posed by the digital environment. In a concurrence, Justice Sotomayor opined:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[180]

Since *Jones* leaves room for interpretation, it seems that the third-party doctrine may not be invoked in the invisible handshake scenario. Imagine that the police did not issue a warrant for surveillance against Jones, but instead, his phone company voluntarily provided his GPS location. If such a case presented itself, it might constitute a violation of the Fourth

---

174 *See* United States v. Miller, 425 U.S. 435, 442–43 (1976).

175 *See generally* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431 (2013).

176 United States v. Jones, 132 S. Ct. 945 (2012). In *United States v. Jones*, the Court inquired whether the attachment of a Global Positioning System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constituted a search or seizure within the meaning of the Fourth Amendment. *Id.* at 948.

177 *Id.* at 949.

178 *Id.*

179 *Id.* at 954 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

180 *Id.* at 957 (Sotomayor, J., concurring) (internal citations omitted).

Amendment. Much ambiguity, however, lies within this scenario as well.

The invisible handshake in NSA programs is far more complex than the scenario in *Jones*. First, the data is not intentionally disclosed by data subjects, nor is it proactively collected by online intermediaries. Instead, comprehensive data is routinely aggregated by online intermediaries as an integral part of their operation.[181] The sharing of such bulks of data, with third parties or government agents, may not involve any action on behalf of the government, the likely defendant in a suit, and therefore may not be considered a search in the first place. Another problem in applying the Fourth Amendment in this case is that rights under the Fourth Amendment are treated as "personal rights," and these rights may not be asserted vicariously.[182] Thus, it is highly impractical to sue the NSA or online intermediaries for any alleged voluntary disclosure of information unless an individual can prove that her own communications have been intercepted. Due to the invisible nature of the partnership, any such attempt could be futile.

Overall, the constitutional protections are limited in their ability to secure civil liberties under the new type of PPP. Private entities are not subject to constitutional limits on searches and are subject to no duty to respect free speech or other fundamental rights. This may leave citizens without any effective remedies against such actions. Statutory limitations on federal laws have the potential to provide such remedies, yet these limitations have ultimately proven insufficient thus far.

B. Statutory Limitations

FISA was originally passed to prevent the unauthorized domestic surveillance programs that occurred prior to its enactment.[183] FISA prohibits the government from engaging in electronic surveillance, or using information obtained by electronic surveillance not authorized by the law (or an express statutory authorization).[184] If the NSA conducts surveillance

---

[181] SCHNEIER, *supra* note 46, at 14–19.

[182] *See* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978); ACLU v. NSA, 493 F.3d 644, 673 (6th Cir. 2007).

[183] *See* 123 CONG. REC. 15,222 (1977) (Statement of Senator Kennedy) (arguing that FISA would "at long last place foreign intelligence electronic surveillance under the rule of law"); Donohue, *supra* note 157, at 782 ("From the beginning, Congress made it clear that the legislation was designed to prevent precisely the types of broad surveillance programs and incursions into privacy . . . .").

[184] 50 U.S.C. § 1809 (2012); Executive Order 12,333 permits the government to target foreigners abroad for surveillance outside of FISA. *See* Exec. Order No. 12,333, 3 C.F.R. pt. 2.1 (1981).

outside of the statutory framework, it could be deemed illegal. While unbound by constitutional restraints, private companies do have limitations on what they can do with the information they control, both under U.S. law and, when operating outside the United States, under international trade agreements.[185]

Congress enacted several laws to ensure the protection of information obtained by private companies, and to govern the usage of this information by governmental agencies. While there are various forms of restriction,[186] the most relevant here are set by the Electronic Communications Privacy Act (ECPA),[187] which is divided into three titles: the Wiretap Act,[188] the Stored Communications Act,[189] and the Pen Register Act.[190]

The ECPA regulates three types of communications: wire, oral, and electronic.[191] Under the ECPA, two permitted exceptions for foreign intelligence surveillance activities exist:[192] activities within the definition of "electronic surveillance" under FISA[193] and non-electronic surveillance involving the acquisition

---

[185] U.S. companies could be generally obligated to various rules when operating outside the United States, although trade agreements could provide exceptions for such obligations. Accordingly, after Snowden's revelations, the European Parliament called for a "Full Review" of the data transfer agreement, which allows a number of U.S. companies to transfer data about EU citizens to the United States. *See* Susan Ariel Aaronson & Rob Maxim, *Data Protection and Digital Trade in the Wake of the NSA Revelations*, 48 INTERECONOMICS 281 (2013) (discussing data protection in the wake of the NSA revelations).

[186] For example, following the Supreme Court Decision in *United States v. Miller*, Congress passed the Right to Financial Privacy Act of 1978 which provided "modest statutory protection for customer financial records held by financial institutions." NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 32 (2008); *see* Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3641 (1978) (codified at 12 U.S.C. §§ 3401–3422 (2012)).

[187] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 42 U.S.C. § 3711 (2012)).

[188] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012).

[189] Stored Communications Act, tit. II, 18 U.S.C. §§ 2701–2711 (2012).

[190] Pen Register Act, ch. 206, 18 U.S.C. §§ 3121–3127 (2012).

[191] For more on the ECPA, see for example, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1278–89 (2004).

[192] 18 U.S.C. § 2511(2)(f) (2012).

[193] *Id.* § 1801. "Electronic surveillance" is defined in FISA as

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication; . . . (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication; . . . (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, . . . or; (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication.

of foreign intelligence information from international or foreign communications.[194] This "exclusivity provision"[195] applies to surveillance conducted under FISA or of foreign communications. But what society can learn from the NSA programs is that not all of the NSA's practices—including, inter alia, the public-private partnership—fall under these exceptions. Therefore, the ECPA applies in the context of the PPP. Both sides are subject to the legal limitations set forth in the ECPA, and particularly, in the Wiretap Act and the Stored Communications Act.

The Wiretap Act applies to real-time, in-transit communications.[196] The Wiretap Act generally prohibits interception of "wire, oral, or electronic communication,"[197] and provides two exceptions for online intermediaries to legally assist the government in intercepting electronic communications.[198] Online intermediaries can authorize real-time interception of electronic communications on their systems, without a court order or certification by the Attorney General, when it is relevant to a computer trespasser investigation. In order to qualify for this exception, four conditions must be satisfied: (1) the online intermediary must authorize the interception; (2) the intercepting person must be lawfully engaged in an investigation; (3) the intercepting person must have reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (4) the interception must be confined to the communications sent or received by trespasser.[199]

Prior to the Cybersecurity Act,[200] the disclosure of stored information and metadata was governed primarily by the Stored Communications Act (SCA).[201] The SCA prohibits the voluntary disclosure of customer communications or records with some exceptions.[202] The law prohibits "provider[s] of remote computing service or electronic communication service[s]" from knowingly divulging "a record or other information pertaining to a

---

Id. § 1801(f). Although companies' voluntary disclosures of information are not surveillance per se, they could be treated as such.

194 *See* LIU, *supra* note 70, at 2–3.

195 *Id.* at 2.

196 18 U.S.C. §§ 2511–2522.

197 *Id.* § 2511(1)(a).

198 *Id.* § 2511(2)(a)(ii)(A)–(B). The two exceptions include (1) "a court order directing such assistance" or (2) where the Attorney General has provided a certification "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." *Id.*

199 *Id.* § 2511(2)(i); Birnhack & Elkin-Koren, *supra* note 12, at 44–45.

200 Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015) (codified at 6 U.S.C. §§ 1501–1510 (2012)).

201 Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

202 *Id.* § 2702.

subscriber to or customer of such service . . . to *any governmental entity*."[203] The law provides several exceptions to this prohibition:[204] Voluntary disclosure of customer communications or records is permitted, inter alia[205] (1) "with the lawful consent of the customer or subscriber"; (2) to a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime; and (3) "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of [communications/]information relating to the emergency."[206] Each of the relevant exceptions should be scrutinized separately.

The first exception is the consent of the *c*ustomer or *s*ubscriber. Contract law governs the relationship between companies and their customers or subscribers. Usually, when an individual signs up for a service or visits a website, he is bound to an agreement with the provider of the service.[207] Such an agreement could enable its owner to use customer information and transfer it to any third party, at any time. This is not far from the current reality for many online services. Some companies explicitly indicate their prerogative to use any data obtained from their customers. For example, Microsoft's policy, which applies to the e-mail services of Hotmail, is to disclose information (including e-mail contents) only (1) to comply with the law; (2) to protect the rights or property of Microsoft or their customers; or (3) to an act on a good faith belief that *such access or disclosure is necessary to protect* the personal safety of Microsoft employees, customers or *the public*.[208] Thus, Microsoft can disclose information to the government at its own discretion, especially if law enforcement agencies request the information due to national security concerns grounded in, inter alia, the protection of the public.

Contracts, however, fall short in addressing the threats of public-private collaboration in surveillance to the civil liberties of

---

[203] *Id.* § 2702(a)(3) (emphasis added).

[204] *Id.* § 2702(b)–(c).

[205] Unlike voluntary disclosure, in the case of an order requiring disclosure of customer communications or records, the government needs either to obtain a warrant, present an administrative or grand jury subpoena (with notice to the subscriber), or obtain a court order for disclosure (with notice to the subscriber). *See id.* § 2703(a)–(b).

[206] *See id.* § 2702(b)–(c).

[207] *See, e.g.*, Ed Bayley, *The Clicks That Bind: Ways Users "Agree" to Online Terms of Service*, ELEC. FRONTIER FOUND. (Nov. 16, 2009), https://www.eff.org/files/2016/03/15/eff-terms-of-service-whitepaper.pdf [https://perma.cc/V4CP-SV8H].

[208] *Microsoft Online Privacy Statement*, MICROSOFT, https://privacy. microsoft.com/en-us/privacystatement [https://perma.cc/J8GD-V4ZA]; Solove, *Digital Dossiers*, *supra* note 36, at 1099.

users of online intermediaries. For one thing, many individuals do not really have a choice. If they wish to partake in society, they must "plug in."[209] Users must subscribe to an Internet Service Provider, open accounts with cable companies, phone services, and e-mail providers, and use search engines and social media.[210] Furthermore the available mechanisms for delivering notices and acquiring users' consent, such as click-through or browse-wrap consent, do not reflect a meaningful choice by end-users who are either unaware of their consent or do not understand the terms of these contracts.[211] Therefore, these contracts fail to signal real preferences of users, which are essential for the market to evolve efficiently.[212] These are often contracts of adhesion that, even though enforceable, rest on a rather shaky legal basis.[213]

Moreover, although the law might restrict the company's ability to transfer its customer's data to the government,[214] it does not forbid the selling of this information to a non-governmental agent. Such restrictions would have a negative effect on the business models of many online intermediaries, which are mostly based on collecting, processing, and selling data.[215] Therefore, this "fourth party" can transfer the data to the government free from legal constraints.[216]

The second exception is inadvertently obtained content that pertains to crime commission. A provider is entitled to divulge the contents of a communication to a law enforcement agency if the contents were obtained unintentionally and appear to pertain to the commission of a crime.[217] Generally, some

---

[209] *See* Solove, *Digital Dossiers*, *supra* note 36, at 1089 (describing the Information Age characteristics).

[210] *Id.*

[211] Margaret Jane Radin, *Taking Notice Seriously: Information Delivery and Consumer Contract Formation*, 17 THEORETICAL INQUIRIES IN L. 515, 515–16 (2016).

[212] *See generally* Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2014).

[213] Generally, terms of service are enforceable, even if non-negotiable. Nonetheless, terms of service are not without limitations and could be considered unconscionable in some cases. *See* Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 606–07 (E.D. Pa. 2007) (holding that the "Second Life" Terms of Service's arbitration provision was unenforceable); Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 178–79 (2011); Ty Tasker & Daryn Pakcyk, *Cyber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 79, 90–92, 115–18 (2008).

[214] *See supra* notes 201–206.

[215] Bagley, *supra* note 213, at 163 ("Google's profit model is based on offering free services to consumers in exchange for their consent to non-negotiable terms of service.").

[216] *See* Michaels, *supra* note 53, at 918, 930 ("[T]he Stored Communications Act prohibits certain telecommunications providers from voluntarily giving information to the government, but allows them to transfer the same information to other private entities. Those entities, in turn, can readily sell or give the information to the government.").

[217] 18 U.S.C. § 2702(b)(7) (2012).

information obtained by online intermediaries is purposefully gathered, and thus is not governed by this exception. Other than that, any information which was obtained inadvertently should at least appear to pertain to the commission of a crime. Bulk data does not generally fall under this category. Rather, it only applies to information regarding a specific individual whom the government has grounds to believe has committed a crime. Thus, sharing bulk information with the government could not fall under this category, as only its analysis could determine whether the content pertained to crime commission.

The third and final exception is emergency. A provider is also entitled to divulge the contents of a communication to a governmental entity, if he believes in good faith that "an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[218] Whether the invisible handshake will fall into the emergency exception, which requires an immediate danger of death or serious physical injury, is debatable.[219] Arguably, the need to conduct ongoing surveillance is due to the constant state of emergency caused by the threat of terrorism. But overall, it is more likely that the emergency exception is not designed for ongoing programs, such as the NSA's, but rather for specific incidents involving an immediate danger of death or serious physical injury.[220]

Arguably, the Cybersecurity Act provides some clarity on sharing some forms of information.[221] Under the Act, private entities are authorized to monitor their information systems, operate defensive measures, and share "cyber threat indicators" or "defensive measures" for a cybersecurity purpose.[222] While the first two components raise many concerns,[223] the third element is most relevant to PPPs. While the Act places some restrictions on information sharing,[224] it mainly forms a framework for

---

[218] *Id.* §§ 2702(b)(8), (c)(4).

[219] *Id.* §§ 2702(b)(8), (c)(4).

[220] *Id.* § 2702(b)(8) ("[A]n emergency involving danger of death or serious physical injury to any person . . . .").

[221] *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015) (codified at 6 U.S.C. §§ 1501–1510 (2012)).

[222] *Id.* § 104.

[223] *See, e.g.*, Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws [https://perma.cc/KT2R-ZBRM] (raising concerns regarding the Cybersecurity Act language).

[224] For example, prior to information sharing, the network operator must remove "any information not directly related to a cybersecurity threat" that the operator "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual." *See* Consolidated Appropriations Act § 104(d)(2)(A).

voluntarily sharing "cyber threat" information with the Department of Homeland Security, which can share such information with any governmental agency, including the NSA.[225] Accordingly, online intermediaries are now able to legally share a "cyber threat indicator"[226] for a "cybersecurity purpose," and in exchange, they are granted immunity from liability in any cause of legal action against them and exemption from any related requests under the Freedom of Information Act.[227]

Currently, there is much ambiguity regarding the Cybersecurity Act. For example, what constitutes a *cyber threat indicator*, and what is a "cybersecurity purpose"? Even with its vagueness, it clearly relates to information regarding cyber activities. What is also clear is that the Cybersecurity Act makes some forms of PPPs legal and much easier to create. It removes most obstacles for PPPs, allowing information sharing between companies and the U.S. government. But the invisible handshake represents more than that. It represents the sharing of bulk data, which could relate to anything and anyone. Hence, while the Cybersecurity Act does provide some clarity—and perhaps mostly immunity for private entities—regarding information sharing, it does not directly regulate the invisible handshake. What one could argue is that the Cybersecurity Act clarifies limitations on private companies: If they are sharing information without a "cyber threat indicator," then it would be illegal for them to monitor their information systems, operate defensive measures, and perhaps most important here, voluntarily share information with the government. Under such an assumption, the Cybersecurity Act effectively makes some voluntary sharing of information illegal. Yet the triggers that authorize voluntary information sharing—"*a cyber threat indicator*" or "*defensive measure*"—are too broadly defined.[228] Most importantly, the new law authorizes the voluntary disclosure of information to further

---

[225] *Id.*

[226] The term "cyber threat indicator" is defined as "information that is necessary to describe or identify" any of the following items or any combination of them:

> malicious reconnaissance . . . ; a method of defeating a security control or exploitation of a security vulnerability; a security vulnerability . . . ; a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; the actual or potential harm caused by an incident . . . ; [or] any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law.

Id. § 102(6).

[227] *Id.* § 105(d)(3).

[228] *See id.* § 102(6), (7).

cybersecurity in general, not necessarily only the security of online intermediaries' own networks, but possibly also the security of other networks.[229]

Snowden's revelations forced the state to seek ways of bringing PPPs under the rule of law. The Cybersecurity Act reflects an attempt to legalize and incentivize information sharing between online intermediaries and the government. Yet the law leaves much room for interpretation by online intermediaries in exercising their discretion. Therefore, in the absence of judicial review, the civil rights of online users are practically subject to the informal understandings between the government and online intermediaries.

IV. SOCIAL AND LEGAL INTERVENTIONS

The invisible handshake worked well for both the government and the private sector under a veil of secrecy.[230] From the government's perspective, PPPs provide operational flexibility and immunity from political and legal sanctions.[231] Operating without any form of oversight clearly enhances any agency's abilities. It also benefitted online intermediaries. For example, under such partnerships, companies could obtain government contracts.[232] Online intermediaries depend on governments for other reasons too. For instance, the government could decide whether the intermediaries are subject to tax and

---

[229] *See* Kerr, *supra* note 223.

[230] The identities of the government's private partners in PRISM are considered its most sensitive secret. Gellman & Poitras, *supra* note 112. As noted in a leaked NSA report: "98 percent of PRISM production is based on Yahoo, Google and Microsoft; we need to make sure we don't harm these sources." *Id.*

[231] *See* Michaels, *supra* note 53, at 906, 922–26.

[232] Many telecommunications companies have contracts with the government, which could be financially crucial for their business models. Reports indicate that Qwest, a major telecommunications company that refused handing warrantless customers' information to the NSA, was pressured by them, inter alia, by suggesting that such action will negatively affect their chances to get future classified work with the government, and/or by adhering to patriotism. *See* Cauley, *supra* note 127. A former Qwest executive alleged later that the government withdrew opportunities for contracts worth hundreds of millions of dollars due to Qwest's refusal to participate in such PPP with the NSA. *See* Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, WASH. POST (Oct. 13, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html [https://perma.cc/BQC5-F288]. The private sector could also use the knowledge and capabilities of the government for its own benefit. For example, the Washington Post reported that Google sought the help of the NSA to aid in cybersecurity measures. *See* Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, WASH. POST (Feb. 4, 2010), http://www. washington post.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html [https:// perma.cc/ HJ9A-DWY3].

antitrust regulation,[233] or if they require a license or a franchise to operate.[234] Clouds of data, however virtual, and computing facilities could also be considered critical infrastructure that may depend on (physical) protection by the state.

Most importantly, there is a shared interest between online intermediaries and governments, and the discrepancy is narrower than often assumed. Governments are commonly entrusted with a regulatory function to promote social welfare: to intervene in economic activity in the case of a market failure, and to secure civil liberties. Yet, as governments become more dependent upon data generated by users of online intermediaries for governance and law enforcement purposes, they develop a stake in facilitating more collection of data.

Online intermediaries are part of the data industry. The logic of the data industry requires maximizing exclusive control over data. Google, Amazon, Twitter, and Facebook strive to offer free services, innovative features, and competitive content, in order to maximize opportunities for collecting massive amounts of personal data.[235] The logic of accumulation mandates that all online activities be recorded and analyzed to optimize the quality of data generated by such companies, and refine its accuracy for advertisers.[236] Therefore, the forces driving the data market are similar to those felt by the government—in order to be effective, both require robust and comprehensive data collection. That is where "surveillance capitalism," as coined by Shoshana Zuboff,[237] meets the *surveillance state*.

The secrecy of the informal collaboration between online intermediaries and governments serves the interest of both. Indeed, if users fear surveillance, they will abstain from some services, which in turn, will reduce the potential for data

---

[233] Google and other American technology companies are currently facing many regulatory challenges over taxation and antitrust matters. On taxation, EU officials are currently reexamining a tax settlement with Google, the British government, and other EU states, and is considering imposing a blockwide standard for taxation. James Kanter & Mark Scott, *Taxing Google and Other U.S. Giants Is Dividing Europe*, N.Y. TIMES (Jan. 28, 2016), http://www.nytimes.com/2016/01/29/business/international/taxing-google-and-other-us-giants-is-dividing-europe.html [https://perma.cc/SCD7-PK36]. On antitrust, EU's antitrust chief formally charged Google of abusing its dominance in web searches. Kelly Couturier, *How Europe Is Going After Apple, Google and Other U.S. Tech Giants*, N.Y. TIMES (Sept. 27, 2016), http://www.nytimes.com/interactive/2015/04/13/technology/How-Europe-Is-Going-After-U.S.-Tech-Giants.html?_r=0 [https://perma.cc/KWR5-VGU8].

[234] *See* Birnhack & Elkin-Koren, *supra* note 12, at 24–25.

[235] For more on how massive amounts of personal data are being routinely collected by companies in exchange for free services, see Claire Porter, *Little Privacy in the Age of Big Data*, GUARDIAN (June 20, 2014), https://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-data [https://perma.cc/B2TW-5V75].

[236] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 79 (2015).

[237] *Id.* at 77.

collection. If users are unaware of surveillance, they are more likely to generate data that is economically valuable to online intermediaries and might also become useful for public safety and national security. Moreover, the invisibility of the handshake between the government and online intermediaries shielded the latter from pushback by consumers. It has also legally protected those intermediaries from lawsuits by their customers and reduced potential vulnerability to shareholder lawsuits.[238]

While the mutual interests of online intermediaries and governments under PPPs are acknowledged, what is lacking under PPPs is the reassurance that the government is not misusing its power.[239] The existence of PPPs without any oversight endangers democracy.[240] Preserving civil liberties and the rule of law necessitates expanding the scope of internal and external oversight.[241] That is, if the government obtains more power, there is a need for greater restraints. Society needs some restrictions and oversight on how data is collected and shared. Such checks and balances could be market-based, regulatory, or both.[242]

---

[238] Jon Michaels suggests other explanations to "why a firm may agree to an informal relationship," for example "structural flaws in corporate decision making." *See* Michaels, *supra* note 53, at 926–27.

[239] *See* Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L., ETHICS & PUB. POL'Y 247, 251 (2005) ("The American people must be confident that the power they have entrusted to NSA is not being, and will not be, abused.").

[240] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1318 (2004) [hereinafter Swire, *The System of Foreign Intelligence Surveillance Law*] (listing examples of secret surveillance use against political opponents in the United States). Generally, flow of information from the private sector to government could impose a chilling effect on democracy. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 39 (1996) ("[T]otalitarian regimes in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control."); Solove, *Digital Dossiers*, *supra* note 36, at 1084–85 (arguing that increasing amount of personal information flowing to the government "can result in the slow creep toward a totalitarian state"); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 471–72 (1999).

[241] Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 240, at 1340 ("To give one example, broad surveillance might be accompanied by greater external oversight.").

[242] Jon Michaels proposed mandating corporate insistence on being served with the requisite instruments of legal compulsion; corporate disclosures describing the nature of the collaborations to Congress and to the inspectors general of the agencies conducting the operations; and escalating burdens of proof that require agencies periodically to demonstrate to the FISA court the continuing utility of ongoing operations. *See* Michaels, *supra* note 53, at 951–65.

A. Social Intervention: Market-Driven Solutions

The current legal framework enables the secrecy of the PPP. Lacking knowledge of the NSA programs, the market was incapable of responding. Once the invisible handshake became more visible, market forces could have played a role in restraining PPPs. Presumably, if consumers became more involved, they could pressure the government and companies to resort to better practices within the existing legal framework. Private technology companies linked to PPPs were placed in a difficult position: while PPPs could be beneficial for them, their alleged involvement in these practices might harm them financially.

Consumers became aware of the *invisible handshake* mostly after Snowden's revelations, which could have potentially harmed online intermediaries by alienating their subscribers, and subsequently jeopardizing their profits.[243] Fearing such potential alienation, which could lead to financial loss, companies that were allegedly involved in PRISM and upstream collection sought to distance themselves from the image of state agents or collaborators.[244] Major private technology companies embarked on a campaign against state surveillance and the negative impact on their customers. For example, because companies were often prohibited from disclosing data requests from government agencies,[245] Twitter (which was not involved

---

[243] For Cisco's alleged financial losses linked to Snowden revelations, see Christopher Mims, *Cisco's Disastrous Quarter Shows How NSA Spying Could Freeze US Companies Out of a Trillion-Dollar Opportunity*, QUARTZ (Nov. 13, 2013), http://qz.com/147313/ciscos-disastrous-quarter-shows-how-nsa-spying-could-freeze-us-companies-out-of-a-trillion-dollar-opportunity [https://perma.cc/AGK7-HSBL]. For IBM's, see Dimitra Kessenides, *IBM Shareholder Sues the Company over NSA Cooperation*, BLOOMBERG BUSINESSWEEK (Dec. 13, 2013), http://www.businessweek.com/articles/2013-12-13/ibm-shareholder-sues-company-over-nsa-cooperation [https://perma.cc/94B8-2FVK].

[244] Although the scope of possible revenue loss is unclear and could vary among various companies, few companies made estimations of the possible financial loss after the revelation of PRISM. For example, the Information Technology and Innovation Foundation (ITIF) estimated that the low-end costs for the U.S. Cloud Computing Industry could be $21.5 to $35 billion. *See* DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 3 (2013), http://www2.itif.org/2013-cloud-computing-costs.pdf [https://perma.cc/8T83-BUVR]; Andrea Peterson, *NSA Snooping Could Cost U.S. Tech Companies $35 Billion over Three Years*, WASH. POST (Aug. 7, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/07/nsa-snooping-could-cost-u-s-tech-companies-35-billion-over-three-years [https://perma.cc/NT7V-928S] (citing the ITIF report).

[245] There are several types of prohibitions. First, the FBI is authorized by section 2709 of the Federal Stored Communications Act to issue NSLs to electronic communication service providers. Such NSLs compel the recipients to disclose "subscriber information and toll billing records information" upon a certification by the FBI that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. §§ 2709(a)–(b) (2012). The recipient of the NSL shall not disclose "to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect

in PRISM) filed a lawsuit in federal court designed to enable them to publish full transparency reports indicating the exact number of national security letters (NSLs) and FISA court orders received.[246] Another example is that of Apple, which released new "Legal Process Guidelines" for U.S. law enforcement agencies,[247] and has also actively opposed legislation and court orders[248] that could weaken security and enable backdoors.[249] Moreover, after Snowden's revelations, several major U.S. technology companies formed the Global Government Surveillance Reform (GGSR),[250] which seeks to further regulate "government surveillance of individuals and access to their information."[251] At the same time, however, there is a growing concern that online intermediaries are being hypocritical in this debate and are merely paying lip service to the defense of civil liberties.[252]

---

to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records." *Id.* § 2709(c)(1). Second, recipients of court orders are obliged to provide the government with "all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy." 50 U.S.C. § 1805(c)(2)(B) (2012). In addition, unauthorized disclosures of national defense information under certain circumstances could result in criminal sanctions, 18 U.S.C. § 793 (2012); some companies sign nondisclosure agreements, and FISC can impose such nondisclosure obligations. For these arguments, see Twitter, Inc. v. Holder, No. 14-cv-04480-YGR, 2016 WL 1729999 (N.D. Cal. May 2, 2016).

246 *See Twitter*, 2016 WL 1729999.

247 *See Legal Process Guidelines: U.S. Law Enforcement*, APPLE (Sept. 29, 2015), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/2Q7Y-SLZM].

248 On February 16, 2016, Apple was ordered by the United States District Court for the Central District of California to help the FBI get into the iPhone used by the San Bernardino shooter Syed Farook. *See* Orin Kerr, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case (Part 1)*, WASH. POST (Feb. 18, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1/?tid=a_inl [https://perma.cc/847S-PDBR]. The FBI needed Apple's aid in this incident as the "auto erase" function was turned on, meaning that if the FBI attempted to guess the passcode ten times incorrectly, the data would be destroyed by encryption. *Id.* The problem was that Farook's iPhone used the iOS9 operating system which could not be decrypted even with a warrant. *Id.* Hence, the court ordered Apple, under the All Writs Act, to create a backdoor into the iPhone or to exploit a potential existing backdoor in their design. *Id.* In response, Apple chief executive Tim Cook publicly stated that Apple intended to fight the court order. *Id.*

249 See for example, in the UK, Alex Hern, *Apple Calls on UK Government to Scale Back Snooper's Charter*, GUARDIAN (Dec. 21, 2015), http://www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill [https://perma.cc/4JCV-MMDR].

250 As of February 15, 2016, these companies include AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo!. *See Global Government Surveillance Reform*, REFORM GOV'T SURVEILLANCE, https://www.reformgovernmentsurveillance.com [https://perma.cc/9LGV-RG3T].

251 *Id.*

252 Facebook, for example, was accused that while it had "been lauded as opposing" the Cybersecurity Information Sharing Act (CISA), which would grant it legal immunity for information sharing with the government, its lobbyists were actually "welcoming CISA behind closed doors." *See* Cory Doctorow, *Petition: Facebook Betrayed Us by Secretly Lobbying for Cyber-Surveillance Bill*, BOING BOING (Oct. 24, 2015), http://boingboing.net/2015/10/24/petition-facebook-betrayed-us.html [https://perma.cc/ACC8-D8KF].

Aside from these types of company reactions, there are other possible market-driven solutions that the private sector could deploy. Online intermediaries could actively fight against the legality of the NSA practices or the constitutionality of the statutes under which these programs purportedly operate. Such a move could enhance companies' reputations and restore their customers' faith. In that sense, companies could also collaborate and fight together for more transparency.[253]

Online intermediaries can also play a more active role in the FISC process, and challenge FISC decisions by filing petitions.[254] Presumably, if companies actively engaged in the FISC process, then FISC might cease its "rubber stamping"[255] of agencies' requests, as judges might be more cautious about issuing blank orders. This could increase transparency to some extent, as the public could better assess whether their information is bluntly shared with the government. But such solution is only partial. Companies could misuse this mechanism by objecting to FISC decisions superficially, merely for the sake of appearance. Moreover, even if companies truly resisted FISC decisions, the existence of other PPPs between them and the government could remain hidden. That is, secret PPPs may still exist under other mechanisms even while consumer trust could potentially be restored by a belief that companies are actively fighting against government agencies.

In addition, online intermediaries could improve transparency of governmental practices. One way to achieve such transparency is to publish transparency reports that provide data on government requests. The problem, however, is that companies are often prohibited from disclosing data requests from government agencies.[256] There are a few ways to bypass such disclosure prohibitions, at least to some extent. Currently, companies are permitted to disclose the number of

---

[253] Such form of a market-driven solution was proposed by a collaboration of various groups, under the title "Reset the Net." RESET THE NET, https://www.resetthe net.org [https://perma.cc/4PP5-46RD]. This initiative calls on everyone (except the NSA) to "build[ ] proven security into the everyday Internet" and "spread NSA-resistant privacy tools." *Id.* Under this initiative, website owners will implement security protocols such as HTTPs, HSTS, and PFS (perfect forward secrecy). *Id.* Mobile App developers will add SSL and certificate pinning, including for "third party code like ad networks and analytics." *Id.* Other companies will also implement a security action plan. *Id.* Finally, even regular users could promote and disseminate privacy tools. *Id.*

[254] 50 U.S.C. § 1861(f)(2)(A)(i) (2012).

[255] *See infra* note 289.

[256] Zack Whittaker, *How Tech Companies Use Warrant Canaries to Secretly Communicate with You*, ZDNET (Mar. 5, 2015), http://www.zdnet.com/article/warrant-canary [https://perma.cc/2VXL-XUEP].

secret data demands in ranges.[257] The problem is that 0 and 999 requests are treated equally.[258] Companies are still prohibited from disclosing the fact that they did not receive any requests from law enforcement agencies.[259]

Interpreting speech in this context, i.e., what constitutes disclosure of requests, led to a bypassing mechanism. Some companies interpreted the legal framework as allowing them to inform the public that they have not received any requests, and companies used unique non-speech methods often referred to as "canaries" in order to do so. For purposes of transparency, several groups formed the Canary Watch,[260] a website that tracks, documents, and lists canaries. A warrant canary is a "published statement that a[n] [online] service provider has not received legal process that it would be prohibited from saying it had received, such as a national security letter."[261] The process is simple: when companies publish a canary, the website informs the public. Then, the same website reports its disappearance, from which the public can infer that the company received secret orders from an intelligence or law enforcement agency.[262] Canaries currently fall into a legal gray area and do not necessarily align with the prohibitions set by the law.[263]

Canaries exemplify a market-driven solution that could lead to higher transparency. The problem is that not all companies use canaries. If a company initially does not inform the public that it has not received a request from the government, the public is unable to infer when they do. Therefore, a canary watch requires the cooperation of private entities. Moreover, even if some companies do list canaries, and the public notices their disappearance, the public is still in no position to know the content of the government's warrant. It could be a specific warrant, designed to locate a single communication for a short, defined period, or it could broadly apply to the entire communication of a company for a long period.

Finally, companies could better secure their products. They could implement encryption technologies that would make communication invisible and inaccessible to them. Under this scenario, companies will not be able to turn over any information regarding their clients, even under a court order. This solution,

---

257 *Id.*

258 *Id.*

259 *Id.*

260 *See* CANARY WATCH, https://canarywatch.org [https://perma.cc/F59K-E5X2].

261 *Id.*

262 *About Canary Watch*, CANARY WATCH, https://canarywatch.org/about.html [https://perma.cc/6THJ-3MFE].

263 *See* Whittaker, *supra* note 256.

however, is successful so long as the government does not prohibit such strong encryption. Despite various regulatory attempts,[264] there are currently no regulatory requirements for the method of encryption at any level. But such regulations could arise, especially if policymakers fear that some companies will embed strong encryption tools into their services. One example of such fear can be traced to January 2015, in which British Prime Minister David Cameron announced that "he would pursue banning encrypted messaging services if Britain's intelligence services were not given access to the communications."[265] Encryption, however, is not a perfect solution. Encryption could be costly and does not necessarily align with the revenue models of companies. They rely on unencrypted information as part of their business models.[266] Furthermore, PPPs could still exist even with encryption, and their secrecy could be well hidden from the public.

If private companies are truly not involved in the government's alleged use of "backdoors," then they should find better ways to secure their products. Such backdoors could negatively affect U.S. companies in the international market, as customers might fear that U.S. technology products are not trustworthy.[267] Cisco announced that they are now shipping equipment to addresses unrelated to a customer, in order to reduce the possibility of the NSA tampering with their products.[268] It is not a perfect solution, as the NSA can still use other PPPs in the supply chain, such as DHL or FedEx, to install backdoors in their products. But Cisco's move still reduces the probability that their products contain backdoors, and more

---

[264] For example of such attempts, see Birnhack & Elkin-Koren, *supra* note 12, at 87 n.195.

[265] Mark Scott, *British Prime Minister Suggests Banning Some Online Messaging Apps*, N.Y. TIMES (Jan. 12, 2015), http://bits.blogs.nytimes.com/2015/01/12/british-prime-minister-suggests-banning-some-online-messaging-apps/?_r=0 [https://perma.cc/G4FP-YMRW].

[266] *See, e.g.*, Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 INT'L DATA PRIVACY L. 200, 206 (2012) ("For instance, at least some cloud providers have business models that gain revenue based on access to unencrypted data, such as Gmail's automatic scanning of the content of email in order to serve targeted advertisements."). Google's essence is information. The name Google is "a play on the word 'googol'" "as a reflection of the sheer volume of information that exists in the world." *Corporate Information*, *Company Overview*, GOOGLE, http://www.google.com/corporate/index.html [https://perma.cc/FY9E-DZSM]; Stephanie A. DeVos, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 173, 190 (2010).

[267] Jeremy Kirk, *To Avoid NSA, Cisco Gear Gets Delivered to Strange Addresses*, CIO (Mar. 19, 2015), http://www.cio.com/article/2899854/to-avoid-nsa-cisco-gear-gets-delivered-to-strange-addresses.html [https://perma.cc/S4P2-QC5Z].

[268] *Id.*

importantly, it signals to their customers that they are not a part of a PPP with the NSA.[269]

Other market-driven solutions could arise from civil society, that is, non-governmental organizations and institutions that manifest the interests and will of citizens. NGOs and individuals could, just like companies, actively fight against the legality of NSA practices and/or challenge the constitutionality of the statutes in court.[270] They could also sue companies to force them to reveal their practices to their consumers. Even if companies acted lawfully, the fear of PPP exposure could change their practices. Finally, watchdog groups could notify the public about companies' interactions with government actors. One example of this is the before-mentioned Canary Watch; but there are others. For example, the Electronic Frontier Foundation (EFF) operates a Secure Messaging Scorecard, designed to rate the applications that secure communications between users.[271] If a company provides an encrypted messaging service, while another does not, end users could choose the former.

End users could also play an important role in cyber safety. Organizations such as the EFF provide surveillance self-defense methods on their website.[272] The website includes an online guide, currently available in three languages, to "defending yourself and your friends from surveillance by using secure technology and developing careful practices."[273] Self-protection in this era might be more important than imagined. Even if the U.S. government adopts an optimal regime, which balances national security threats with liberties, other jurisdictions might not act accordingly. Thus, protection from overall surveillance that relies on state actors, or even companies and NGOs, will not suffice. Therefore, end users should adopt email encryption technologies such as Pretty Good Privacy (PGP)[274] or GNU Privacy Guard

---

[269] *Id.*

[270] For an overview of litigation against the NSA surveillance programs, see Kara Brandeisky, *NSA Surveillance Lawsuit Tracker*, PROPUBLICA (July 10, 2013), http://projects.propublica.org/graphics/surveillance-suits [https://perma.cc/Y282-VW4P] (last updated May 13, 2015).

[271] *See Secure Messaging Scorecard*, ELEC. FRONTIER FOUND., https://www.eff.org/secure-messaging-scorecard [https://perma.cc/ZRY9-3G2X].

[272] *See Surveillance Self-Defense*, ELEC. FRONTIER FOUND., https://ssd.eff.org [https://perma.cc/2XSY-HRRW].

[273] *Id.* This website is currently available in English, Arabic, and Spanish.

[274] "Pretty Good Privacy or PGP is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files." *See* Margaret Rouse, *Pretty Good Privacy (PGP)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy [https://perma.cc/95FY-MJJX].

(GPG),[275] use anonymous browsing tools such as the TOR network,[276] or even engage in physical or digital protests.[277]

As history shows, there are two problems that arise from reliance on market-driven solutions as a single check on the abuse of power: (1) the public tends to forget, and (2) companies do not have incentives to challenge PPPs without public pressure. Snowden was hardly the first whistleblower who revealed NSA programs. The public learned of other NSA programs in 2006,[278] but that did not stop the NSA or the companies from collaborating, or continuing to collaborate, after such revelations. The post-Snowden era tells a similar story. While market forces might have driven both the government and companies to provide more information on the nature of their PPPs, it mainly—and limitedly—yielded some information on the secret FISC decisions.[279] Social intervention (either via the market, or by civil society) is, therefore, a limited tool for providing proper checks and balances, and legal intervention by policymakers is required.

B. Legal Intervention

The nature of distributed networks presents challenges to the ability of the state to govern effectively. The government's response to this governance crisis was to acquire some control over information flow. To achieve such control, the United States worked—almost simultaneously—along two strategies. One strategy was to acquire ongoing access to bulk data via informal collaborations with online intermediaries.[280] Part III showed that this strategy created a legal twilight zone and left big holes

---

[275] "OpenPGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures. This document specifies the message formats used in OpenPGP." *See* Network Working Grp., *OpenPGP Message Format*, INTERNET ENG'G TASK FORCE (Nov. 2007), http://www.ietf.org/rfc/rfc4880.txt [https://perma.cc/4D4T-GXV5].

[276] The Onion Router (Tor) is a network connected "through a series of virtual tunnels . . . allowing both organizations and individuals to share information over public networks" with less surveillance risks. *See Tor: Overview*, TOR PROJECT, https://www.torproject.org/about/overview.html.en [https://perma.cc/7ZFX-NVCM].

[277] An example of such digital protest took place on February 11, 2014, under the title: "The Day We Fight Back." *See* Jessica Mckenzie, *Tomorrow the Internet Puts Collective Foot Down to Say 'No' to Mass Surveillance*, TECHPRESIDENT (Feb. 10, 2014), http://techpresident.com/news/24735/tomorrow-internet-puts-collective-foot-down-say-no-mass-surveillance [https://perma.cc/PU6W-E6QF]. In that protest, more than 5000 websites displayed a banner that read "Dear Internet, we're sick of complaining about the NSA. We want new laws that curtail online surveillance." *Id.* "Stop Watching Us" is another example of such initiative. *See Stop Watching Us*, STOP WATCHING US, https://optin.stopwatching.us [https://perma.cc/QUV6-M628].

[278] *See supra* note 133.

[279] *See infra* Section IV.B.1.

[280] *See supra* Section II.B.

in the legal shield meant to secure civil rights. Another strategy for acquiring access to information flow was a *regulatory approach*, whereby enforcement agencies could obtain information from online intermediaries subject to legal oversight. This section analyzes the limits of current regulatory tools in safeguarding human rights and liberties.

1. Judicial Oversight

Information-gathering programs were placed under various forms of oversight by the legislative, judicial, and executive branches.[281] Congress, the Intelligence Oversight Board (within the Executive Office of the President), the Office of Intelligence Policy and Review (Department of Justice), the Assistant to the Secretary of Defense for Intelligence Oversight and the Office of General Counsel (Department of Defense), and finally the FISC are all reviewing NSA activities to some extent.[282] Under this regulatory approach, executive agencies were placed under the supervision of the other branches: the legislature, which attempted to craft the rules of information gathering, and the judiciary, tasked with ruling on what information could be divulged.[283]

As Snowden's revelations showed, this regulatory approach was flawed. Prima facie, the FISC was meant to serve as a gatekeeper of American citizen's liberty. But this was hardly true. A report to Congress on FISC requests in 2012 revealed that the government filed 1,789 applications for authority to conduct electronic surveillance.[284] Only one request was not approved, and this was due to the government's withdrawal.[285] Between 1979 and 2012, there were 33,949 "Traditional FISA Surveillance Orders."[286] Only eleven were rejected.[287] FISC judges had almost indefinitely complied with government agencies' surveillance requests, and granted blank

---

[281] *See* Hayden, *supra* note 239, at 252–54 (describing the oversight framework, while focusing on legislative, executive, and judicial oversights).

[282] *Id.*

[283] *Id.*

[284] *See* Letter from Peter J. Kadzik, Principal Deputy Assistant Att'y Gen., U.S. Dep't of Justice, to Hon. Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf [https://perma.cc/BE2J-EHQ6].

[285] *Id.*

[286] *See Foreign Intelligence Surveillance Act Court Orders 1979–2014*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/wiretap/stats/fisa_stats.html [https://perma.cc/38MB-HL4D].

[287] *Id.*

orders.[288] Thus, the judicial process established under FISA has proven an inadequate safeguard of rights and liberties because the FISC effectively rubber-stamped bulk data requests by governmental agencies.[289]

One of the main deficiencies of the FISC process is tied to its secrecy. Generally, upon receiving a FISC order, any person may challenge the order's legality by filing a petition.[290] Due to the secrecy of FISC orders, the only "persons" eligible to challenge FISC orders are the companies that received them.[291] The problem is that online intermediaries have very little incentive to challenge these orders,[292] and therefore, only a few

---

[288] A good example of such warrants is that of Verizon. This large American telecommunications provider was required by a blanket order to provide metadata on all telephone calls in its systems on an "ongoing daily basis." *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], No. BR 0605 (FISA Ct. May 24, 2006). This revelation demonstrated that court orders were not always confined to suspected individuals, or merely against non-U.S. citizens. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/2NCL-CZ27].

[289] It should be noted that some scholars argue that the success rate of government requests in FISC does not imply that FISC serves as a rubber stamp, but rather, that the government only makes requests that would benefit them and that they know FISC judges would approve. One scholar argues that this is partially due to the high costs of filing a FISC request application (in time, resources, and reputation). *See* Conor Clarke, Note, *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). For more on government's success rate in FISC proceedings, see for example, *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 49 (2013) (statement of Laura K. Donohue, Professor, Georgetown University Law Center), http://scholarship.law.georgetown.edu/cong/117 [https://perma.cc/R45G-XPUR] (arguing that the "rather remarkable success rate" raises a "serious question about the extent to which FISC and [the Foreign Intelligence Surveillance Court of Review] perform the function they were envisioned to serve"); Theodore W. Ruger, Essay, *Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 245 (2007) (arguing that the "government success rate [is] unparalleled in any other American court").

[290] 50 U.S.C. § 1861(f)(2)(A)(i) (2012). After filing a petition, a FISC judge conducts an initial review within seventy-two hours. *Id.* § 1861(f)(2)(A)(ii). Upon ruling on whether the petition is "not frivolous," *id.*, either side can seek en banc review before the full FISC, *id.* § 1803(a)(2)(A), or file a petition for review with the FISA Court of Review. *Id.* § 1861(f)(3). Subsequently, both sides may petition for writ of certiorari to review such decision. *Id.*

[291] *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 741 (S.D.N.Y. 2013) (noting that "section 215 does not provide for any person other than a recipient of an order to challenge the orders' legality or otherwise participate in the process").

[292] There are many reasons why private companies would avoid challenging a FISC order. One reason could be financial. The judicial process is expensive and compliance could be cheaper. *See* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 389–90 (2004). Another reason could be that online intermediaries view Courts as agents of the State, and their orders were closely examined to serve an important purpose. An example of a third possible reason is the perceived chances of success. If FISC merely serves as a rubber stamp, companies might refrain from challenging its decisions, as they might assume that there are relatively low chances of success. Thus, these companies conduct a cost-benefit

companies do so.[293] To address the problems that arise from the ex-parte nature of FISC decisions, Congress considered including an independent agency to serve as a special advocacy board in the FISC to reduce the likelihood that the FISC will simply rubber-stamp requests.[294]

The main lesson to be drawn from the regulatory approach under FISA is that courts can only play a limited role in monitoring the exercise of power by governmental agencies in the era of big data. The reason is that governments have adapted strategies to address the governance crises in digital networks. Rather than target particular suspects and pursue a warrant for additional collection of data based on suspicion, the current paradigm reverses the order. It involves collecting and

---

analysis, weighing their chances of success against the perceived (high) costs. *See generally* Peter Siegelman & Joel Waldfogel, *Toward a Taxonomy of Disputes: New Evidence Through the Prism of the Priest/Klein Model*, 28 J. LEGAL STUD. 101, 103 (1999); Clarke, *supra* note 289, at 128 (arguing that "parties tend to do things when they predict that the expected benefits exceed the expected costs"). Moreover, FISA protects private companies to some extent, and it even grants some companies retroactive immunity from liability. Prior to the FAA in 2008, many lawsuits were filed against telecommunications companies for cooperation with the NSA outside of FISA. Eventually, the FAA awarded these companies retroactive immunity from liability and the cases were dismissed. In addition to immunity, the government reimburses any electronic communications service provider for providing information, facilities, or assistance in accordance with the statutory framework. Under this provision, compliance is costless, at least in the monetary sense, and incentivizes companies to comply with FISC orders. *See* 50 U.S.C. § 1881a(h)(2) (2012); Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), *remanded by* 539 F.3d 1157 (9th Cir. 2008).

[293] Although there are some indications that few companies did challenge FISC orders, many others did not. Yahoo!, Lavabit, and Apple apparently fought governmental orders to turn over data. *See* Schneier, *supra* note 143.

[294] Under the proposed bill (which was not enacted), the Privacy and Civil Liberties Oversight Board (PCLOB)—an independent agency that works within the executive branch of the U.S. government to review executive branch actions and ensure a balance with privacy and civil liberties—would have served as a Special Advocate Board in FISC. *See* Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. (2013). Under the proposed bill, PCLOB would appoint:

> (1) attorneys to serve as public interest advocates in proceedings before the Foreign Intelligence Surveillance Court [FISC], a judge of the petition review pool, the Foreign Intelligence Surveillance Court of Review [FISCR], and the Supreme Court under the Foreign Intelligence Surveillance Act of 1978 [FISA]; and (2) technical and subject-matter experts [including experts of computer networks, telecommunications, encryption, and cybersecurity], not employed by the Federal Government, to be available to assist [such advocates] in performing their duties.

Id. The proposed bill required such courts, in any matter "involving a significant interpretation or construction of [FISA]," to appoint at least one public interest advocate who would: (1) "participate fully with the same rights and privileges as the Federal Government;" (2) "represent . . . the interests of the people of the United States in preserving privacy and civil liberties, including with respect to . . . rights . . . under the Fourth Amendment to the Constitution;" and (3) "have access to all relevant evidence" as well as the authority to petition the court to order the government to produce other necessary evidence. *Id.* For another proposition, see also the FISA Court Reform Act of 2013, S. 1467, 113th Cong. (2013).

processing large volumes of data, and applying data analytics to identify patterns and correlations in order to detect suspicious behavior.[295] The use of big data and social media analytics for monitoring threats, predicting harmful activities, and prevention, require access to bulk data. Consequently, it is no longer sufficient to acquire an individual warrant in order the perform law enforcement tasks. This may render conventional legal oversight, which is tailored to authorize data collection based on reasonable suspicion, redundant. The nature of mass surveillance and big data analytics requires blanket orders, and thus calls for a different type of legal intervention to safeguard civil liberties.

2. Promoting Transparency

There are various legal suggestions on how to provide better checks and balances on PPPs.[296] Some suggestions focus on transparency. These strategies assume that insight into the actions of the NSA and private companies could increase oversight. GGSR, for example, has reached a deal with the Obama Administration, allowing companies to disclose more information on the customer data they are compelled to share

---

[295] On the use of predicting strategies based on data analysis for law enforcement purposes, see Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461 (2015); Tal Zarsky, *Governmental Data Mining and Its Alternatives*, 116 PENN. ST. L. REV. 285 (2011).

[296] For example, in an open letter to President Obama and to Members of Congress, GGSR urged the government to reform government surveillance practices worldwide. *See Global Government Surveillance Reform*, *supra* note 250. GGSR claim that they are "focused on keeping users' data secure," and that they are "pushing back on government requests to ensure that they are legal and reasonable in scope." *Id.* GGSR proposes five principles for reform: (1) "[l]imiting [g]overnments' [a]uthority to [c]ollect [u]sers' [i]nformation." This first principle should be achieved by codifying "sensible limitations" on government's "ability to compel service providers to disclose user data that balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the Internet." *Id.* Furthermore, governmental surveillance should be limited "to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications. . . . [and] (2) [o]versight and [a]ccountability." *Id.* This creates strong checks and balances for intelligence agencies seeking to collect or compel the production of information. *Id.* In addition, "[r]eviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry." *Id.* (3) "Transparency [a]bout [g]overnment [d]emands. Governments [will] allow companies to publish the number and nature of government demands for user information," and "promptly disclose this data publicly." *Id.* (4) "Respecting the [f]ree [f]low of [i]nformation . . . Governments should permit the transfer of data and . . . not inhibit access by companies or individuals to lawfully available information . . . stored outside of the country . . . [and] should not require service providers to locate infrastructure within a country's borders or operate locally" (5) "Avoiding [c]onflicts [a]mong [g]overnments." GGSR suggests "a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions . . . [When] the laws of one jurisdiction conflict with the laws of another . . . governments should work together to resolve the conflict." *Id.*

with the government.[297] But this does not apply to PPPs, and therefore does not offer any check on informal collaboration. This "transparency arrangement" discloses the number of national security orders and requests issued to communications providers, the number of customer accounts targeted under those orders and requests, and the underlying legal authorities.[298] In addition, companies will be allowed to publish reports listing the number of security letters they receive from the FBI, and how many customer accounts those letters affect (to the nearest thousand). Some of these orders are subject to a six-month delay, or a two-year delay once a government agency develops a surveillance effort on "a platform, product or service (whether developed or acquired) for which the company has not previously received such an order."[299] Notably, other forms of the invisible handshake, such as "upstream" collection, are not handled through this agreement.[300]

This sort of limited transparency might raise public awareness of the invisible handshake and the sharing of information with governmental agencies. Yet it will likely have only a limited impact; the arrangement permits the government to issue bulk orders. In other words, while a single order might be reported, its scope and potential impact will be concealed. Also, public reports on information sharing with governments might harm the financial interests of online intermediaries by generating mistrust and chilling users away from the service. This may create further incentives for governments and companies to opt for informal information sharing.

---

[297] *See* Spencer Ackerman, *Tech Giants Reach White House Deal on NSA Surveillance of Customer Data*, GUARDIAN (Jan. 27, 2014), http://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data [https://perma.cc/4ETB-NFY3].

[298] What was revealed thus far? Tens of thousands of Microsoft, Google, Facebook and Yahoo! accounts have their data turned over to U.S. government authorities. *See* Ackerman, *supra* note 140. But the precise numbers and types of requests the companies received were not revealed. Furthermore, this information was received via court orders, and we are unaware of the NSA information gathering under Executive Order 12,333, and outside the legal process via the invisible handshake. Which companies announced that they require a warrant for handing out content? An annual report by the EFF on online service provider's privacy and transparency practices regarding government access to user data reveals interesting results. *See Who Has Your Back?*, ELEC. FRONTIER FOUND., https://www.eff.org/who-has-your-back-2014 [https://perma.cc/BQA6-TJ7D]. The EFF examined the announced privacy and transparency practices of twenty-six U.S. companies. *Id.* As for voluntary disclosure of information, the EFF found that prior to 2014, only twelve companies announced that they require a warrant for handing out content. *Id.* Since 2014, however, that number increased to twenty-three companies. *Id.* Which companies still do not specify that a warrant is required to access their content?: AT&T, Comcast, and Snapchat. *Id.*

[299] *See* Ackerman, *supra* note 140.

[300] *Id.*

Others have suggested obligating private companies to file reports that disclose any informal or formal agreement to share or transfer information.[301] Congress, for example, could limit the companies' ability to transfer users' data; increase oversight over the governmental programs;[302] and perhaps even restrict governmental agencies' ability to acquire access to certain types of data. Congress could further implement barriers to information collection (such as time limits on data retention), and require governmental agencies and companies to make full transparency reports to Congress, which could examine whether both sides of these PPPs acted lawfully. But as this article argues, these suggested practices are either inapplicable or may seriously compromise the government's ability to govern. Therefore, governments would be required to acquire information only through bulk orders, which also lack sufficient legal oversight and, therefore, fail to offer a better safeguard to civil liberties.

3. Are Online Intermediaries State Actors?

The informal collaboration of government and online intermediaries generates a legal twilight zone. Prior to the enactment of the Cybersecurity Act, such collaborations were almost entirely outside the reach of the rule of law and the Constitution did not apply to them. Yet the Cybersecurity Act does little to remedy this problem. This regulatory scheme falls short of offering a comprehensive framework for voluntary PPPs, as its vague legal standards leave much discretion to online intermediaries working in the shadow of the law.[303] Therefore, it fails to offer proper checks and balances. This legal framework merely grants immunity to private companies, allowing them to either begin, or continue, to collaborate with the government.

A partial solution for bringing PPPs under the rule of law would be to treat private companies that divulge information to the government as state actors.[304] As state

---

[301] Jon Michaels proposed to require corporations to file reports under seal, to members of the House and Senate intelligence and judiciary committees and to the inspector general of the participating government agency, summarizing any agreement "to share or transfer information about U.S. persons to military or intelligence agencies." *See* Michaels, *supra* note 53, at 952–53.

[302] As Jon Michaels proposed, increasing the current data Congress currently receives, along with holding hearings to investigate programs, could solve part of the problems emerging from current PPPs. *See id.* at 953–57.

[303] *See supra* Section III.B.

[304] For a broader discussion of the state action doctrine, see Daphne Barak-Erez, *A State Action Doctrine for an Age of Privatization*, 45 SYRACUSE L. REV. 1169 (1995); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503 (1985); Ira Nerken, *A New Deal for the Protection of Fourteenth Amendment Rights: Challenging*

actors, the actions of online intermediaries under the invisible handshake are not only made visible, but are also subject to the principles of the Constitution—mainly, the First and Fourth Amendments. Treating private companies as state actors will require transparency and oversight. Those private companies cannot receive full immunity for sharing information with the government and would be subject to review and constitutional scrutiny.[305] Knowing that their actions as state actors are subject to review and constitutional scrutiny, companies may alter their data-sharing practices.

Pragmatically, however, even if private companies are treated as state actors, holding them accountable for their actions will be fairly difficult: as long as PPPs are kept secret, the odds of imposing liability are extremely low. Note that even after Snowden's revelation on the involvement of nine Internet companies in PRISM, there was no actual proof of their participation in such a program.[306]

C. Organizational Design

Many of the Congressional efforts to restrain the use of power by the government via PPPs, have focused either on *the scope* of data sharing (e.g., the Cybersecurity Act) or *the process* of obtaining data (e.g., FISA orders). These attempts fail to recognize the increasing reliance of governments on online intermediaries for effective governance. They assume that governmental agencies will need to access the information flow only occasionally and that such access will be focused on predefined targets—sporadic, and limited in scope. This approach overlooks the governance crisis and the growing dependency of governmental agencies on systematic access to the information flow as a means of governance. This crisis is not tied to a particular emergency or national security crisis. It is essentially the new challenge of governing behavior in a networked information era.

The governance crisis demands new governance tools that will allow governments to perform their duties in a networked

---

the Doctrinal Bases of the Civil Rights Cases *and State Action Theory*, 12 CIV. RTS.-CIV. LIBERTIES. L. REV. 297 (1977).

[305] *See generally* Barak-Erez, *supra* note 304; Chemerinsky, *supra* note 304; Nerken, *supra* note 304.

[306] *See, e.g.*, T.C. Sottek & Joshua Kopstein, *Everything You Need to Know About PRISM*, VERGE (July 17, 2013), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet [https://perma.cc/3WR9-V8A2] ("The companies at the heart of PRISM's controversy are also acting out, but the specific details regarding their involvement in government surveillance on US citizens is still unclear.").

environment. The challenge is to design such measures so that they will not jeopardize the enormous advantages of a free and open information flow. Consequently, the governance crisis may require adjustment of the traditional checks and balances. We must move beyond revising the scope of governmental authority in specific rules, or refining the judicial process to allow more meaningful legal oversight in acquiring bulk data. The governance crisis may require new thinking of the organizational design to allow data sharing and secure civil rights.

For instance, instead of focusing on how to regulate and monitor the acquisition of information, policymakers may focus their attention on the way data is being used after it has been obtained through PPPs. Under this approach, Congress would not place restrictions on the sharing of data but instead on the use of it. Enforcement agencies and companies would not be restricted in their sharing of data to those times where a "cyber threat indicator" of any sort is present. The use of such information by governmental agencies, however obtained, will be strictly regulated and subject to legal oversight.

Oversight might also be reconsidered in terms of organizational design. Oversight should not be limited to self-reporting by online intermediaries, or by governmental agencies furnishing transparency reports to Congress. The implementation of oversight could be achieved by reshaping the organizational design and integrating oversight into the structure and the ongoing process of using the data. When oversight is built into the organizational structure, it may offer a more robust safeguard to civil rights. Oversight, for instance, could be conducted by an impartial entity—external to the executive branch—that is integrated into the process and physically present at intelligence and enforcement agencies. This new function could be tasked with reviewing the agency's day-to-day use of information and internal policies regarding the use of information. Both government agents and the entity tasked with oversight could be held personally liable for any unlawful practices under both civil and criminal law in order to promote accountability. This practice both recognizes the need to obtain bulk data and, at the same time, improves legal certainty by placing limitations on any misuse of data rather than its sharing.

CONCLUSION

Information sharing between governmental agencies and private companies is not likely to cease in the digital age; it is necessary for the new challenges of governance. But a democratic

society cannot allow information sharing practices to occur in a legal twilight zone. If PPP practices will continue in their current form in the United States—and worldwide—then the rule of law and civil liberties might be at risk. To strike a proper balance between national security needs and civil liberties, policymakers must rethink their traditional approaches to legal intervention.

Proposals to increase oversight and transparency fall short of addressing the challenges arising from the need to give the government systematic access to information flow. Such proposals will only aid in upholding the rule of law at the margins. In an era of big data, providing proper oversight through traditional judicial review will be almost impossible; FISC decisions proved that.[307] Calls to increase transparency suffer from similar limitations. Transparency will be difficult to achieve due to the sensitive nature of information and the need to act, at least occasionally, under the veil of secrecy. This inevitability weakens the incentives of public representatives to act vigorously in restraining the use of power by the executive branch as the actions that must be kept secret are rarely politically rewarding. While the use of warrant canaries, or other transparency efforts, should be encouraged, they are insufficient to achieve the level of transparency necessary for upholding the rule of law.

This article argues that in devising policies to address governance by online intermediaries, policymakers should assume that this emerging model of governance is here to stay. Consequently, efforts to restore the checks placed on governmental power should focus on systematic collaboration between governments and online intermediaries. The governance crisis may require new thinking about organizational design in order to allow data sharing while simultaneously securing civil rights. One option, for instance, is for policymakers to focus on the use of information—not the methods by which it was obtained—and impose external oversight by an impartial entity on the use of information by governmental agencies.

The Snowden revelations provoked numerous reform initiatives in an attempt to restore civil rights in a networked information society. These initiatives assumed that the informal collaboration disclosed by Snowden was the exception. Consequently, reform initiatives were mostly patchwork repairs to the existing rules and processes. This type of collaboration is a response to a deeper governance crisis caused by distributed networks, to which the government responded with new modus

---

[307] *See supra* Section IV.B.1.

operandi. Therefore, governance by proxy requires rethinking the current checks on governmental powers.

If the governance crisis deepens, then online intermediaries are likely to face growing pressure to serve as proxies for governance, and the potential risks to our liberties could rise substantially. As such, a proper legal intervention is crucial now for preserving human rights and liberties in the future.