UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 81 ● Winter 2019

REGULATING DATA PRIVACY AND USE: A KEY TO MODERN NATIONAL SECURITY?

David Zwier

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

REGULATING DATA PRIVACY AND USE: A KEY TO MODERN NATIONAL SECURITY?

David Zwier*

I. INTRODUCTION

Cybercrime has been called "the single greatest transfer of wealth in history."[1] Unanswered, as of yet, is the long-term effect that cyber force will have on geopolitical power. This Note first compares the differing approaches to privacy and data regulation between the United States and European Union, and outlines several of the European Union's General Data Protection Regulation ("GDPR")[2] provisions that impact private companies' use of individuals' private data.[3] Next, this Note explores the current cyber security landscape from the United States' perspective, evaluating both current policies and norms.[4] Finally, this Note proposes how a national data and privacy regulation scheme could benefit United States' foreign policy goals.[5]

II. DIVERGENT APPROACHES TO DATA AND PRIVACY REGULATION: UNITED STATES AND EUROPEAN UNION

The United States and the European Union are the two main players internationally when it comes to data and privacy regulation—yet each has taken a

* Candidate for J.D., May 2020, University of Pittsburgh School of Law.

[1] *Future of Warfare Before the S. Comm. on Armed Servs.*, 114th Cong. 3 (2015) (statement of Gen. (Ret.) Keith Alexander, President and CEO, IronNet Cybersecurity), https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf.

[2] Council Directive 95/46 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119).

[3] *See infra* Part II.

[4] *See infra* Part III.

[5] *See infra* Part IV.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

vastly different approach in the area.[6] This Part first looks at the United States' approach to regulating data and privacy and then evaluates the regulatory scheme in the European Union under the recently implemented GDPR.

The United States seeks to balance innovation with security from harm,[7] and lacks a national standard when it comes to the use and privacy of data. Different standards apply depending on the type of data or industry involved.[8] As an initial matter, the general regulatory approach to the tech industry has been to err on the side of non-regulation in hopes of encouraging business development and innovation.[9] Therefore, companies' processing of personal data is not limited unless tangible harm results to consumers or it is otherwise against the law.[10] When regulation does occur, it "is likely to be based on ad hoc intuitions of regulators and judges," rather than coherent standards.[11] In some ways, contrary to its intentions, the United States' approach can create uncertainty for businesses. Additionally, this piecemeal approach endangers the personal data of individuals, who might suffer harm or harassment if directly linked to and identified through their personal data.[12] Lastly, the data privacy and security conversation in the United States has historically centered on the due process and individual liberty issues inherent in personal data

[6] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 880–81 (2014).

[7] Stephen R. Miller, *First Principles for Regulating the Sharing Economy*, 53 HARV. J. ON LEGIS. 147, 152–53 (2016).

[8] Schwartz & Solove, *supra* note 6, at 881 (citing DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 404–05 (1992)).

[9] MARINA LAO ET AL., FED. TRADE COMM'N, THE "SHARING" ECONOMY ISSUES FACING PLATFORMS, PARTICIPANTS & REGULATORS 6–7 (2016), https://www.ftc.gov/system/files/documents/reports/sharing-economy-issues-facing-platforms-participants-regulators-federal-trade-commission-staff/p151200_ftc_staff_report_on_the_sharing_economy.pdf.

[10] Schwartz & Solove, *supra* note 6, at 881 (citing Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 913 (2009)).

[11] *Id.* at 897 (citing Carol M. Rose, *Crystals and Mud in Property Law*, 40 STAN. L. REV. 577, 592–93 (1988); Kathleen M. Sullivan, *The Supreme Court 1991 Term—Foreword: The Justices of Rules and Standards*, 106 HARV. L. REV. 22, 57–59 (1992)).

[12] *See* Schwartz & Solove, *supra* note 6, at 899–900 (footnotes omitted).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

and has been colored by the idea that government surveillance is more dangerous than corporate surveillance.[13]

On the other hand, the European Union's default is to require an affirmative legal basis for processing data that can be used to identify individuals.[14] The GDPR codifies this approach and represents an expansive and comprehensive reimagining of previous privacy law.[15] The regulation, which has been in place since May 25, 2018, carries the ideal that "[n]atural persons should have control of their own personal data."[16] The GDPR supersedes the laws of member states and created a uniform European Union standard for personal data.[17] Moreover, the regulation modified or expanded prior laws in significant ways. Outside of well-delineated exceptions, it requires that individuals consent to the collection and use of their data.[18] It also creates individual rights of access to information,[19] data portability,[20] correction,[21] and erasure.[22] Finally, the GDPR curtails profiling individuals based on their personal data.[23]

A. United States' Approach

The United States' privacy rights have developed in two primary categories: First, within the common law system, through challenges to and interpretations of the Fourth Amendment and individual civil liberties over time; and second, through

---

[13] Senator Sheldon Whitehouse, *Why Americans Hate Government Surveillance but Tolerate Corporate Data Aggregators*, LAWFARE (June 2, 2015), https://www.lawfareblog.com/why-americans-hate-government-surveillance-tolerate-corporate-data-aggregators.

[14] Schwartz & Solove, *supra* note 6, at 881.

[15] *See id.* at 885.

[16] General Data Protection Regulation, *supra* note 2, at pmbl. ¶ 7.

[17] Juliana De Groot, *What Is the General Data Protection Regulation? Understanding and Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (July 15, 2019), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

[18] General Data Protection Regulation, *supra* note 2, at ch. II, arts. 6–7.

[19] *Id.* at ch. III, § 2, art. 15.

[20] *Id.* at ch. III, § 3, art. 20.

[21] *Id.* at ch. III, § 3, art. 16.

[22] *Id.* at ch. III, § 3, art. 17.

[23] *Id.* at ch. III, § 4, art. 22.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

statutes and regulations.[24] Although the former category is more prevalent in current discourse, which often focuses on governmental surveillance and data collection, the latter category carries greater relevance to the current discussion of privacy and data regulations.[25]

Prior to the Fair Credit Reporting Act of 1970, no statute protected the privacy rights of individual citizens.[26] While the Fair Credit Reporting Act protects individuals from the actions of corporations, it only covers specific subject matter.[27] Subsequent examples of this approach are the Video Privacy Protection Act of 1988, which prevented "disclosure of personally identifiable rental records of 'prerecorded video cassette tapes or similar audio visual material,'"[28] and the Cable Television Consumer Protection and Competition Act of 1992, which regulated all data associated with individual cable subscribers.[29]

In 1997, as the commercial potential of the Internet was becoming apparent, then-President Bill Clinton issued the Framework for Global Electronic Commerce.[30] The Clinton administration, seeking to balance future innovation against security from harm for individuals, directed the Department of Commerce to regulate the emerging Internet economy.[31] In doing so, the Department of Commerce was to set up a regulatory scheme where businesses and market leaders would play a significant role in developing Internet-related regulations.[32] The approach taken in the Framework for Global Electronic Commerce set the tone for data and privacy

---

[24] *See generally*, Daniel J. Solove, *A Brief History of Information Privacy Law*, PROSKAUER ON PRIVACY, PLI (2006) (surveying the relevant privacy statutory and regulatory frameworks).

[25] *See id.*

[26] *See id.*

[27] *See id.*

[28] *Video Privacy Protection Act*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/vppa/ (last visited Oct. 31, 2019).

[29] *Cable Television*, FED. COMMC'NS COMM'N, https://www.fcc.gov/media/engineering/cable-television; *see also Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (This Rule limited the amount of information that could be gathered about and from children.).

[30] Mark Hall, *ICANN International Organization*, ENCYCLOPEDIA BRITANNICA (Oct. 11, 2017), https://www.britannica.com/topic/ICANN#ref1080889.

[31] *Id.*; *see* Stephen R. Miller, *First Principles for Regulating the Sharing Economy*, 53 HARV. J. ON LEGIS. 147, 152–53 (2016).

[32] Hall, *supra* note 30.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

regulation by encouraging businesses to self-regulate when addressing privacy concerns.[33] In response, industry standards and codes, as well as organizations like the Online Privacy Alliance, were developed.[34]

The sharing economy, which has arisen in the past ten years and is entirely based online, provides a striking illustration of how the Clinton administration's policy for self-regulation continues to hold sway today. Both federal and state regulators have struggled to strike the innovation-security balance when it comes to the sharing economy.[35] The Federal Trade Commission ("FTC") plays a significant role in regulating the sharing economy.[36] However, the FTC's approach, as evidenced in its 2016 report, is to refrain from regulation because the "sharing economy is still evolving, and to regulate it now would be to curtail its innovative potential."[37] In 2017, for example, the FTC entered into two consent agreements with Uber, one for $20 million for false advertising regarding driver compensation,[38] and the other for a 2014 data breach of customer and driver information.[39] The false advertising consent decree is notable in that it represents the same approach taken by the FTC to regulate brick-and-mortar retailers.[40] While the order on data security relates to modern privacy, it does not impose any restrictions on Uber's use of customer data, and only addresses security breaches.[41]

The regulatory actions against Uber have likely done little to change its collection and use consumer data.[42] Moreover, the FTC's efforts to change companies' behavior through fines appears to be ineffectual and faces criticism for

[33] *Id.*

[34] *Id.*

[35] Alice Armitage et al., *Design Thinking: The Answer to the Impasse Between Innovation and Regulation*, 2 GEO. L. TECH. REV. 3, 5 (2017) (footnotes omitted); *see* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1678 (2017) (footnotes omitted).

[36] *See* Calo & Rosenblat, *supra* note 35, at 1678 (footnotes omitted).

[37] *Id.* at 1678 n.294 (citing LAO ET AL., *supra* note 9, at 5).

[38] *Id.* at 1678 (footnote omitted).

[39] *Id.* at 1678 (citing *In re* Uber Techs., Inc., No. 152-3054, 2018 WL 1836645 (F.T.C. Apr. 9, 2018)).

[40] *See id.* at 1678–79.

[41] *Id.* at 1678 (citing *In re* Uber Techs., Inc., No. 152-3054, 2018 WL 1836645 (F.T.C. Apr. 9, 2018)).

[42] Calo & Rosenblat, *supra* note 35, at 1627–28.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

taking too light a touch.[43] The FTC's five-billion-dollar fine of Facebook for violating a 2012 consent order was the largest FTC fine of a tech company to date; tellingly, Facebook's stock rose after the fine was announced.[44] Although some recent FTC penalties have been larger, the fines of European Union privacy regulators dwarf them.[45]

These practices are especially concerning because there are significant questions about consumers' comprehension of how companies like Uber use their data.[46] Likewise, individuals may not understand the magnitude of personal data collection nor how that data is used. A 2013 ACLU report evaluating data transparency listed privacy as a primary concern for mobile device users.[47] The report outlines that most American online consumers are misinformed about the "nature and extent of [data collected]."[48] Many of those consumers think that companies are required to obtain their consent to gather data[49] and are unaware of the ways they can limit data collection.[50] Critically, when consumers understand how

[43] Brian Barrett, *Fines Alone Aren't Enough to Slow Down Big Tech*, WIRED (Sept. 9, 2019), https://www.wired.com/story/youtube-ftc-fines-alone-arent-enough/.

[44] Peter Kafka, *The US Government is Fining Facebook $5 Billion for Privacy Violations, and Wall Street Thinks That's Great News*, VOX (July 12, 2019), https://www.vox.com/recode/2019/7/12/20692434/facebook-5-billion-fine-ftc-privacy-regulation.

[45] *Compare Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented, *with* Ana Zarzalejos, *The 7 Biggest Fines the EU Have Ever Imposed Against Giant Companies*, BUS. INSIDER (July 19, 2018), https://www.businessinsider.com/the-7-biggest-fines-the-eu-has-ever-imposed-against-giant-corporations-2018-7.

[46] ACLU CAL., LOSING THE SPOTLIGHT: A STUDY OF CALIFORNIA'S SHINE THE LIGHT LAW 2–4 (2013), https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California%27s%20Shine%20the%20Light%20Law%20final.pdf.

[47] *Id.* at 2 (citing Kristina Knight, *Mobile Consumers Most Concerned About Privacy*, BIZREPORT (Apr. 27, 2011), http://www.bizreport.com/2011/04/survey-mobileconsumers-most-concerned-about-privacy.html).

[48] *Id.* at 3 (quoting FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[49] *Id.* at 2 (footnote omitted).

[50] *Id.* at 2 (citing KRISTEN PURCELL ET AL., PEW RESEARCH CTR., SEARCH ENGINE USE 2012: SUMMARY OF FINDINGS (Mar. 9, 2012), https://www.pewresearch.org/internet/2012/03/09/search-engine-use-2012/).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

their data is collected, used, and shared, they take action.[51] According to a Pew study, "[f]ifty-four percent of smartphone users have decided not to download an application upon discovering how much personal information they would need to share to use it, and 20 percent have uninstalled an application upon learning it collected more personal information than they wanted to share."[52] Another potential concern is that companies such as Uber can use data from a position of market dominance to profile and steer consumers in particular directions.[53]

Lately, however, there are indications that some states are unhappy with the status quo of companies self-regulating the use of individuals' private data. California, for one, appears to be following the lead of the European Union's GDPR with the California Consumer Privacy Act of 2018.[54] Although California's law is somewhat more limited in scope than the GPDR, it represents a significant step towards a different approach to data privacy in the United States due to the size of California's economy and the location of many tech companies within its borders.[55] Vermont is another state that has stepped into the arena, albeit more gingerly, with a regulation on the use of individuals' personal data by third-party data brokers.[56] On the federal stage, FTC commissioners recently advocated before the House Energy and Commerce subcommittee on consumer protection for greater power to regulate privacy and data security.[57] However, until Congress acts or a critical mass of states lead companies to change their approach nationally, it appears unlikely that the

[51] *Id.* at 3 (citing Jeff John Roberts, *Privacy as the Next Green Movement? Study Says Companies Will Compete on Data Practices*, GIGAOM (July 29, 2013), http://gigaom.com/2013/07/29/privacy-as-the-next-green-movement-study-sayscompanies-will-compete-on-data-practices/).

[52] *Id.* at 3 (citing JAN LAUREN BOYLES ET AL., PEW RESEARCH CTR., PRIVACY AND DATA MANAGEMENT ON MOBILE (Sept. 5, 2012), https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/).

[53] Calo & Rosenblat, *supra* note 35, at 1651 (citing Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014)); *see also* ACLU CAL., *supra* note 46, at 7–8.

[54] *See* Samuel D. Goldstick et al., *Ringing in 2019 with New State Privacy and Data Security Laws Impacting Data Brokers and Insurers*, NAT'L L. REV. (Jan. 10, 2019), https://www.natlawreview.com/article/ringing-2019-new-state-privacy-and-data-security-laws-impacting-data-brokers-and.

[55] California Consumer Privacy Act of 2018, 55 CAL. CIV. CODE § 2 (West 2018).

[56] VT. STAT. ANN. tit. 9, §§ 2430, 2433, 2446, 2447 (2017).

[57] Cecilia Kang, *F.T.C. Commissioners Back Privacy Law to Regulate Tech Companies*, N.Y. TIMES (May 8, 2019), https://www.nytimes.com/2019/05/08/business/ftc-hearing-facebook.html (quoting FTC chairman Joseph Simons: "We urge Congress to enact privacy and data security legislation, enforceable by the F.T.C.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

United States approach to privacy and data security will shift from a deferential self-regulatory approach.

B. Europe's Approach

The European Union's approach to privacy and data security diverges starkly from that of the United States. The divergence stretches back to 1948, decades before the Internet, when the United Nations General Assembly adopted the Universal Declaration of Human Rights ("UDHR").[58] Outlining fundamental human rights with World War II as a backdrop,[59] Article 12 of the UDHR states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[60] With the rise of the Internet, the concept of an individual right to privacy was combined with the idea of personal data protection within the European Union.[61]

As a consequence, the European Union starts with the assumption that the right to privacy is fundamental,[62] which in turn creates an environment where European governments can be more proactive in protecting this right for its citizens.[63] Tellingly, privacy rights are enumerated in the constitutions of several European Union member states.[64] Additionally, the European Convention on Human Rights guarantees "the right to respect for . . . private and family life, . . . home and . . .

---

[58] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UDHR].

[59] *History of the Document*, UNITED NATIONS, http://www.un.org/en/sections/universal-declaration/history-document/index.html (last visited Apr. 21, 2018).

[60] UDHR, *supra* note 58, at art. 12.

[61] Thomas Shaw, *Privacy Law and History: WWII-Forward*, INT'L ASS'N OF PRIVACY PROF'LS (Mar. 1, 2013), https://iapp.org/news/a/2013-03-01-privacy-law-and-history-wwii-forward/.

[62] Schwartz & Solove, *supra* note 6, at 880. The historical underpinnings of data protection within the European Union, digital or otherwise, lie in the World War II era use of citizens' personal data by the Nazi's Gestapo forces and the Soviet's KGB forces. Alvar Freude & Trixy Freude, *Echoes of History: Understanding German Data Protection*, BERTELSMANN FOUND. (Oct. 1, 2016), http://www.bfna.org/research/echos-of-history-understanding-german-data-protection/; *see* Charles Maynes, *Snowden Revelations Lead Russia to Push for More Spying on Its Own People*, PUB. RADIO INT'L (Dec. 4, 2013), https://www.pri.org/stories/2013-12-04/russia-uses-snowden-excuse-step-spying-its-own-people.

[63] Shaw, *supra* note 61.

[64] *See, e.g.*, GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND, [BASIC LAW] May 23, 1949, BGBL. 1, art. 1 (establishing guarantees of personhood and human dignity, from which derive the rights of informational self-determination); CONSTITUCIÓN ESPAÑOLA [CONSTITUTION] Dec. 27, 1978, art. 18 (establishing a right to personal and family privacy as well as limits on data processing).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

correspondence."[65] Overall, the European Union's approach questions the ability of "market forces" to properly address social issues when compared to effective legislation.[66]

This backdrop led to the adoption the GDPR as broad European Union-wide protections for data privacy and security.[67] The GDPR also creates significant individual rights. Individuals have a right to transparency[68] and access to their data.[69] Transparency entails having clarity as to when and to what extent an individual's personal data is being collected and used either in the present or future.[70] Furthermore, "the specific purposes for which personal data are processed should be explicit . . . and determined at the time of the collection."[71] This precludes the collection of personal data for an indefinite purpose.[72] The preamble adds, "in particular . . . the period for which personal data are stored is limited to a strict minimum."[73] Access to data gives an individual the right to know "whether or not personal data concerning him or her are being processed," the right to know the purposes, categories, storage period or criteria, and whether they are subject to profiling.[74]

---

[65] EUROPEAN CONVENTION ON HUMAN RIGHTS, CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS, ROME, 4.XI.1950, art. 8; *see also* EU CHARTER OF FUNDAMENTAL RIGHTS, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, http://fra.europa.eu/en/charterpedia/article/0-preamble (framing privacy and data protection rights as critical in light of societal changes and developments in technology).

[66] David Lazarus, *Europe and U.S. Have Different Approaches to Protecting Privacy of Personal Data*, L.A. TIMES (Dec. 22, 2015), https://www.latimes.com/business/la-fi-lazarus-20151222-column.html; *see also* Mehreen Khan & Jim Brunsden, *EU to Demand Tough Data-Protection Rules with Future Trade Deals*, FIN. TIMES (Feb. 9, 2018), https://www.ft.com/content/e489abba-0dc5-11e8-8eb7-42f857ea9f09.

[67] General Data Protection Regulation, *supra* note 2, at ch. III, § 1, art. 12; pmbl. ¶ 39.

[68] *Id.*

[69] *Id.* at ch. III, § 2, art. 13; pmbl. ¶ 39.

[70] *Id.* at ch. III, § 1, art. 12; pmbl. ¶ 39.

[71] *Id.*

[72] *Id.*

[73] *Id.* at pmbl. ¶ 39.

[74] *Id.* at ch. III, § 2, art. 15.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

Other individual rights created under the rules are the right to data portability,[75] correction,[76] and erasure.[77] Portability requires that, upon request, an individual receive their personal data "in a structured, commonly used and machine readable format and have the right to transmit those data to another" without interference.[78] Correction allows individuals to demand their data be up to date and mistake free.[79] The right to erasure, or right to be forgotten, empowers individuals to require the elimination "of personal data concerning him or her without undue delay" in certain circumstances.[80] Erasure is allowed when the "data are no longer necessary in relation to the purposes for which they were collected or . . . processed," or where the individual withdraws their consent or objects to the processing.[81]

Consent is foundational to the GDPR and will likely be the primary way companies collect and process individuals' data.[82] Under these Rules, an individual's data may be processed "only if and to the extent that" he or she has provided consent, or in one of five other limited situations.[83] Consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes," and be provided through "a statement or by a clear affirmative action."[84] Additionally, a written request for consent "shall be presented . . . in an intelligible and easily accessible form, using clear and plain language."[85] Moreover, an individual can "withdraw his or her consent at any time," and the process for withdrawal must "be as easy" as giving consent.[86] The text accompanying the rules clarifies that "[s]ilence, pre-ticked

[75] *Id.* at ch. III, § 3, art. 20.

[76] *Id.* at ch. III, § 3, art. 16.

[77] *Id.* at ch. III, § 3, art. 17.

[78] *Id.* at ch. III, § 3, art. 20.

[79] *Id.* at ch. III, § 3, art. 16.

[80] *Id.* at ch. III, § 3, art. 17.

[81] *Id.*

[82] *See* Sheera Frenkel, *Tech Giants Brace for Europe's New Data Privacy Rules*, N.Y. TIMES (Jan. 28, 2018), https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html.

[83] General Data Protection Regulation, *supra* note 2, at ch. II, art. 6.

[84] *Id.* at ch. I, art. 4, ¶ 11.

[85] *Id.* at ch. II, art. 7(2).

[86] *Id.* at ch. II, art. 7(3).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

boxes or inactivity should not . . . constitute consent," and "[w]hen the [data] processing has multiple purposes, consent should be given for all of them."[87]

The GDPR also has a special concern for personal data that is processed through automated decision-making or used for profiling.[88] This right is emphasized by its incorporation throughout many other individual rights.[89] The right to be free from profiling extends to personal indicators such as "economic situation, health, personal preferences or interests . . . a location or movements" among others.[90] In cases of consent to the profiling and automated decision-making, the individual retains the right to "obtain human intervention."[91]

The GDPR has not only affected the business practices of companies within the European Union, but also the way that companies treat the data of United States consumers.[92] For example, companies such as Facebook and Google are already updating their privacy policies and terms of service in advance of the GDPR's implementation date.[93] Also, certain product rollouts were pulled back from the European Union market.[94] Thus, it is fair to say that companies' prior policies of collection and use of personal data will almost certainly be revised or curtailed. It is still too early to know entirely how companies within the European Union will adapt their businesses to the GDPR, what changes they will also apply in the United States, and the unforeseeable effects that the regulations will have.

Given the extent to which tech companies such as Uber, Google, Facebook, and Airbnb have lobbied against data regulations in the United States, it seems unlikely they will willingly apply the GDPR's personal data standards wholesale to their United States activities.[95] Although proposals to regulate data use have so far failed to gain traction in the United States Congress, there appears to be renewed bipartisan

---

[87] *Id.* at pmbl. ¶ 32.

[88] *Id.* at ch. III, § 4, art. 22; pmbl. ¶ 71.

[89] *Id.* at ch. III, § 4, art. 22; pmbl. ¶ 71.

[90] *Id.* at pmbl. ¶ 71.

[91] *Id.*

[92] *See* Frenkel, *supra* note 82.

[93] *Id.*

[94] *Id.*

[95] *E.g.*, Armitage et al., *supra* note 35, at 29 (footnotes omitted).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

interest in moving a proposal forward.[96] Also, state regulations such as the California Consumer Privacy Act may lead companies to adopt GDPR-like standards of transparency, access, and consent across the United States rather than having multiple conflicting policies based on state regulations.[97]

While it remains unclear if federal regulations will come to bear, or if individual states' regulations will result in companies changing their data and privacy practices wholesale, what is certain is that a regulatory framework for data collection and privacy would upend the current United States' status quo in the arena. Companies using agreements filled with legalese to request consent from customers while also making it difficult for individuals to withdraw consent and terminate the collection of their data might have to change their policies.[98] Additionally, individual consumers would likely have a stronger private right of action against companies than they currently enjoy.[99] The application of the GDPR or similar regulatory regime would, in short, stand the Internet-based tech industry on its head by exposing the vast amount of personal data collected, analyzed, and likely used to profile consumers.[100] As this Note goes on to discuss, regulating the data privacy practices of private companies may carry implications that stretch beyond the rights of individuals.

III. UNDERSTANDING THE CYBERSECURITY LANDSCAPE

Cyberattacks have become a part of daily life. On Friday, September 28, 2018, Facebook announced that a cyberattack exploited a vulnerability in their code, compromising the personal information of nearly fifty million users.[101] Attacks have also reached to the core of American democracy. The most prominent attack—at least within United States intelligence agencies—was Russia's uncontroverted

[96] *See* Cameron F. Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation*, BROOKINGS INST. (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

[97] *See* Goldstick et al., *supra* note 54.

[98] ACLU CAL., *supra* note 46, at 2–3 (citing Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 1, 17 (2008) (describing how long it would take consumers to skim website privacy policies)).

[99] *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

[100] *See, e.g.*, *id.*

[101] Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

hacking and social media cyber campaign to influence the 2016 United States presidential election.[102] For the average person, however, it can be difficult to assess what level of concern they should feel about cyber threats to their personal matters or the United States' national stability.

In the realm of cyber conflict, attackers come "in five distinct varieties: 'vandals, burglars, thugs, spies, and saboteurs.'"[103] Regardless of the attacker's style, the most dangerous threats come from nation-state-backed attackers.[104] The United States faces significant challenges in the cyber realm, which roughly fall into three categories: shaky cyber deterrence, a generalized lack of norms when it comes to the use of cyber capabilities by nation-states, and the United States' failure to embrace a coherent strategy to address the emerging cyber landscape.[105] Although the challenges are intertwined, breaking them apart allows for a more nuanced understanding of the problems.

A. Cyber Deterrence

The United States has been unable to deter cyberattacks against the United States government or private companies. General Paul M. Nakasone, Commander of the United States Cyber Command, "conceded in his [2018] confirmation hearing . . . 'they don't fear us,' . . . admitting that after spending billions of dollars on new defenses and new offensive weapons, the United States has still failed to create a deterrent against cyberattacks."[106] The most dangerous types of attacks are those directly or indirectly backed by rival nation-states such as Iran, North Korea, Russia, and China who can bankroll attackers and shield them from prosecution.[107]

Cyber deterrence is critical because of the significant costs that cyberattacks can have. These costs can include direct losses to governmental entities and private businesses, as well as the lost competitive advantages when adversaries steal

[102] INTELLIGENCE CMTY. ASSESSMENT, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS ii (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[103] DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 2 (2018).

[104] *See id.*

[105] *Id.* at 2, 298.

[106] SANGER, *supra* note 103, at 298.

[107] *Id.*; COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 3–5 (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

intellectual property.[108] It is unsurprising that the United States, the world's largest economy, is the prime target for cyberattacks.[109] According to Michael Sulmeyer, a former Pentagon official who currently runs a Harvard cyber initiative: "When it comes to cyberspace . . . the United States has more to lose than its adversaries because it has gone further in embracing innovation and connectivity without security."[110]

The lack of conversation regarding cyber policy and cyber capabilities is a barrier to creating effective deterrence. Comparing the scope of debate and policy considerations related to the use of nuclear force with the scope of conversation regarding the use of cyber force, it is clear that "[s]o far, there has been no equivalent debate about using cyber weapons."[111] The blame for this lack of discussion could lie squarely at the feet of the United States government. "Naturally secretive, intelligence officials and their military counterparts refuse to discuss the scope of America's cyber capabilities for fear of diminishing" its advantage over adversaries.[112]

Some contend, therefore, that the United States must show its capabilities and willingness to use its cyber weapons for other nations to understand that "there is a price to pay for truly serious cyberattacks."[113] By refusing to take official credit for cyberattacks such as the Olympic Games, or the North Korean "left of launch" missile campaign, the United States fails to link actions and consequences.[114] The positions taken by former military and intelligence officials, such as James E. Cartwright, retired United States General and former Vice Chairman of the Joint Chiefs of Staff, bolster the arguments that such a link is required in order to deter such attacks.[115] For example, Cartwright believes these capabilities must be known

[108] *See generally* COUNCIL OF ECON. ADVISERS, *supra* note 107, at 5–24.

[109] *See* Jade Scipioni, *The Worst Cyber Attacks of the Past 10 Years*, FOX BUS. (Dec. 4, 2018), https://www.foxbusiness.com/features/the-worst-cyber-attacks-of-the-past-10-years; SANGER, *supra* note 103, at 303.

[110] SANGER, *supra* note 103, at 303.

[111] *Id.* at xiv.

[112] *Id.*

[113] *Id.* at 304.

[114] *Id.* (noting acceptance, by many, that these attacks were carried out by the United States); *see also id.* at 274–76, 296–98.

[115] *Id.* at 31–32.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

to achieve deterrence, "[b]ecause if you don't know it's there, it doesn't scare you."[116] The message is that establishing red lines in cyberspace will help deter cyberattacks.

Still, an unanswered question is whether to engage in the preemptive use of cyber force. In the past two years, the United States has displayed an increased willingness to use offensive cyber capabilities.[117] This shift is evidenced in the United States Cyber Command's 2018 testimony to Congress that "[t]he United States must increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage[s]."[118] However, the risk is that "hacking the hackers" amounts to engaging in a constant war on the enemy's turf.[119] Such a shift in strategy begs the question asked by Kenneth Todorov, a retired Air Force Brigadier General: "Are we, as a military and a nation . . . prepared to go after potential targets in advance? And if so, are we ready for other nations to do the same to us?"[120]

B. Lack of Norms

The second category of challenges the cyber realm suffers is a general lack of norms. Currently, "the cyber world still operate[s] with almost no internationally accepted rules of behavior . . . countries, terrorists, and tech companies constantly test[] the boundaries with few repercussions."[121] Clear cyber norms are essential to address the risks of a cyber conflict escalating into analog warfare or a cyberattack directed at infrastructure placing the world economy and lives of civilians in danger.[122]

However, the United States faces two significant hurdles to establishing norms that govern cyberattacks and cyberwar—a lack of willingness to swear off United

---

[116] *Id.*

[117] WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 20–21 (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[118] SANGER, *supra* note 103, at 301.

[119] *Id.*

[120] *Id.* at 278.

[121] *Id.* at 60.

[122] MARTIN C. LIBICKI, CRISIS AND ESCALATION IN CYBERSPACE 36–37, 97–99 (2012).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

States offensive capabilities and a lack of trust in other nation-states.[123] Theoretically, neither challenge is insurmountable. While "[n]o [c]ountry likes giving up military or intelligence capabilities," it can be argued that "we have done it before."[124] For example, "America swore off chemical and biological weapons when we determined that the cost to civilians of legitimizing them was greater than any military advantage they offered . . . limit[ing] the kinds of nuclear weapons we would build, and bann[ing] some."[125] Thus, some argue it is plausible that "[w]e can do the same in cyberspace, but only if we are willing to openly discuss our capabilities and to help monitor cyberspace for violators."[126] According to Jack Goldsmith, a Harvard law professor who served in the George W. Bush Justice Department, the missing ingredient for establishing cyber norms "is the United States government's failure to look in the mirror."[127] So long as the United States refuses to give up or promise not to use its cyber weapon capabilities, rival nations are unlikely to abandon their cyber arsenals.[128]

Another problem is the United States government's inability to keep a handle on their own cyber weapons, which not only reduces their deterrent capability, but also puts businesses and individuals at risk.[129] One poignant example is the Stuxnet worm used in the Olympic Games attack against Iran that escaped into the broader cyber world after being deployed, causing broad losses.[130] Another is Shadow Brokers' theft or leak of a significant number of National Security Agency ("NSA") cyber weapons such as EternalBlue, which played a key role in the 2017 WannaCry

[123] SANGER, *supra* note 103, at 305.

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] *Id.* at xxiii.

[128] *Id.*

[129] *See* Matthew Gault, *The U.S. Government Is Utterly Inept at Keeping Your Data Secure*, NEW REPUBLIC (June 12, 2019), https://newrepublic.com/article/154167/government-nsa-inept-protecting-cyber-data-whatsapp.

[130] SANGER, *supra* note 103, at 22–23; Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

and NotPetya attacks.[131] These attacks are estimated to have jointly caused billions in economic losses.[132] Consequently, some argue that if the government cannot keep cyber weapons secret, it might as well broadcast its capabilities to achieve deterrence.[133]

A related issue is the lack of trust between nations competing for cyber power. Speaking about the essentially nonexistent differentiation between intelligence and offensive-focused cyber implants and tools embedded in foreign networks, a senior NSA official said "[w]e can't convince them. And they can't convince us," that an implant is purely for surveillance when it could easily be retooled for offensive purposes.[134] Moreover, when it comes to norms, the United States' foreign policy track record may sap its moral authority.[135] Other countries can easily call out the hypocrisy in American protests about violations of sovereignty since "[t]he United States d[oes] not exactly have clean hands when it c[omes] to influencing elections in other countries."[136] In past decades, the CIA, in the interest of foreign policy and economic interests, targeted elections in Italy and Iran, attempted to kill Fidel Castro in Cuba, and "mount[ed] covert influence campaigns for elections in South Vietnam, Chile, Nicaragua, and Panama."[137] Surmounting this lack of trust will be critical to any effort to establish cyber norms, and may well require the United States to give up actual cyber weapon capabilities in order to create buy-in among potential partners.

C. Lack of Consensus and Coherence on Cyber Strategy

Finally, the United States has faced challenges with strategically comprehending the changing and emerging nature of cyber threats. This subsection explores how broader definitions and understandings of exercising cyber power gave China and Russia key strategic advantages at different times over the United States.

---

[131] SANGER, *supra* note 103, at 227–29, 287–91; Andy Greenberg, *The Untold Story of NotPeyta, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[132] Greenberg, *supra* note 131.

[133] *See* Andy Fitch, *Once the Code Gets Out: Talking to David E. Sanger*, L.A. REV. OF BOOKS: BLOG (Oct. 12, 2018), https://blog.lareviewofbooks.org/interviews/code-gets-talking-david-e-sanger/.

[134] SANGER, *supra* note 103, at 73.

[135] *Id.* at 177–78.

[136] *Id.*

[137] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

The United States government's internal response to Iran's 2011 direct denial of service, or DDoS, attacks on United States' banks demonstrated the struggle to comprehend and respond to cyberattacks.[138] Some government officials saw the incident as "the equivalent of an Iranian submarine coming off the [United States] coast and launching something."[139] Others, however, characterized the incident as "a bunch of Iranians driving down the middle of the street playing a lot of loud music and generally being obnoxious."[140] Although this type of confusion could seem innocuous, it might also represent a failure to grasp that cyber weapons are "not simply a new tool but also what war fighters call a 'new domain': the place where future power conflicts great and small w[ill] play out."[141]

The lack of consensus on the role of cyber defense and force also impacted how the United States organized its cyber capabilities. Initially, United States cyber capabilities were somewhat siloed in the different branches of the military and other government agencies, including the NSA, CIA, and FBI. Whereas other nations, such as Iran, put cyber weapons at the top of their arsenals given how reliant all of modern society has become on electronic networks.[142] Thus, the federal government's creation of United States Cyber Command was one step taken to address past decision-making siloes. However, a broad and coherent strategy for cyber engagement remains elusive.[143]

China's and Russia's approaches to cyber power contrast that of the United States. China "[does] not distinguish between 'economic advantage' and 'national security advantage.' To a country whose power rests on keeping the economy growing, there is no such distinction."[144] This approach is juxtaposed to that of the United States, which counters that it "breaks into foreign networks only for

[138] *See id.* at 50–51.

[139] *Id.* at 50.

[140] *Id.*

[141] *Id.* at 12.

[142] *Id.* at 43, 48.

[143] Mack DeGeurin, *U.S. Silently Enters New Age of Cyberwarfare*, INTELLIGENCER (Sept. 11, 2018), http://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html (detailing policy changes between the Obama and Trump administrations regarding the offensive use of cyber force).

[144] SANGER, *supra* note 103, at 70–71.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

'legitimate' national-security purposes,"[145] and differentiates that the intelligence collected is not given "to United States companies to enhance their international competitiveness or increase their bottom line."[146] This principled American distinction did little good when China carried out a prolonged campaign of intellectual property and trade secret theft against the United States.[147] Undoubtedly, China's campaign erased some competitive advantages that United States companies had created through painstaking research and development involving millions of dollars of investments.[148]

Unlike China, Russia was less interested in the theft of trade secrets and intellectual property—rather, Russia approached cyber power as an ongoing campaign in a never-ending cyberwar for global influence.[149] This approach culminated most visibly in the effort to influence the 2016 United States presidential election.[150] The Gerasimov doctrine, which sees the lines between war and peace as blurry or nonexistent, embodies Russia's approach.[151] Under Russia's approach, cyber tools and weapons are not siloed; instead, they are a comprehensive part of constant campaign in which they can be combined and recombined with analog weapons to wage constant war.[152] Thus, to Russians, cyberwar "was all on a spectrum. At one end was pure propaganda. Then came fake news, manipulated election results, the publication of stolen emails. Physical attacks on infrastructure marked the far end."[153]

In the wake of the 2016 election, it became clear that the United States underestimated how potent social media could be as a tool to widen the country's political and social fault lines. One prominent author on the subject says that "[i]n

[145] *Id.* at 70.

[146] *Id.*

[147] *See, e.g.*, Indictment, United States v. Su Bin, No. CR1400731, 2014 WL 10290282 (C.D. Cal. filed Aug. 14, 2014); Indictment, United States v. Wang Dong, No. 14–118 (W.D. Pa. filed May 1, 2014) [hereinafter *Wang Dong* Indictment].

[148] *See Wang Dong* Indictment, *supra* note 147, at 2 (outlining the harm suffered by United States companies from cyberattacks that stood to benefit Chinese companies).

[149] SANGER, *supra* note 103, at 157–58, 190.

[150] INTELLIGENCE CMTY. ASSESSMENT, *supra* note 102, at ii–iii.

[151] SANGER, *supra* note 103, at 157–58.

[152] *Id.*

[153] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

our fixation on the types of cyberattacks we thought we understood—against power grids or banks or nuclear centrifuges—we missed the turn towards manipulating voters."[154] Whereas Russia, with its long history of Soviet propaganda, understood the power that cyber weapons could have to wage a psychological war of attrition on an individual's confidence in their state and sense of personal security.[155] Russia understood that "cyberattacks can be used to undermine more than banks, databases, and electrical grids—they can be used to fray the civic threads that hold together democracy itself."[156]

The two leading global cyber powers, the United States and China, reached an agreement in September of 2015 to curb the use of economic espionage.[157] The agreement came in the wake of hacks by China in preceding years to steal intellectual property, trade secrets, and United States government personnel information, and led to a "marked drop-off in hacking by the Chinese."[158] Thus, the 2015 agreement points toward the potential for norms to affect the way that nation-states interact with each other in the cyber realm. It may also have been a tacit recognition by China that it is quickly transitioning from being a perpetrator of cybercrime to being a target for such attacks. However, the agreement did not grow past the initial two parties, and may now hold little water, given the current trade war between the United States and China.[159]

Nevertheless, the 2015 agreement, and China's role in the global economy, indicate that China will likely be an essential party for any future conversations on cyber norms.[160] Chris Painter, the head of the State Department's cyber unit,

---

[154] *Id.* at 238.

[155] *Id.* at 239.

[156] *Id.*

[157] Ellen Nakashima & Steven Mufson, *The U.S. and China Agree Not to Conduct Economic Espionage in Cyberspace*, WASH. POST (Sept. 25, 2015), https://www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.636e4b6a37dc.

[158] SANGER, *supra* note 103, at 123.

[159] Linnette Lopez, *Trump's Trade War Is Hurting China's Economy, but It's Giving Beijing an Opportunity It Never Dreamed of*, BUS. INSIDER (Nov. 24, 2019), https://www.businessinsider.com/trump-trade-war-tariffs-china-bijing-political-defense-opportunity-2019-11.

[160] *See* KENNETH LIEBERTHAL & PETER W. SINGER, CYBERSECURITY AND U.S.-CHINA RELATIONS, BROOKINGS 32–33 (Feb. 2012); *see also* Nick Leung, *China Brief: The State of the Economy*, MCKINSEY & CO. (Mar. 2019), https://www.mckinsey.com/featured-insights/china/china-brief-the-state-of-the-economy.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

explained this shift in attitude: "[China] looked into the future and saw that 'a few years from now, people are going to be stealing industrial designs from the Chinese.'"[161] In a shift President Trump assumed office, the United States has shown increased speed and willingness to attribute cyberattacks to specific perpetrators.[162]

Ultimately, it is clear that cyber-related issues have had a transformative effect on nearly every area of society. This new reality presents immense challenges; in particular, because cyber weapons have shown they do not discriminate between combatants and non-combatants, and cyber power has allowed nation-states and specific interests to engage in campaigns around the clock.

IV. DATA PRIVACY REGULATION AND FOREIGN POLICY

When it comes to data privacy, the conversation thus far in the United States—in particular, since the Snowden revelations—has focused on the risk of overreach by government surveillance programs.[163] One side of the debate contends that federal data collection programs threaten civil liberties while the other contends that large-scale collection is necessary to monitor for radicalization of extremists across the ideological spectrum and prevent future attacks.[164] This part first outlines how the focus on government surveillance, while perhaps merited, has ignored the scope of data collection by private corporate entities. Second, it explains why, given the breadth of data collection by corporations, it is imperative from a foreign policy perspective that corporations engaged in the collection and processing of individuals' private data have adequate security measures in place and are accountable when they fail to protect the data. Finally, this section suggests that regulating data privacy practices of private corporations could address both the privacy concerns of individuals as well as buttress the United States' strength as a cyber power and thus benefit its foreign policy.

In the United States, the conversation around data and privacy has most visibly focused on the government's data collection programs. The American public is of

[161] SANGER, *supra* note 103, at 123.

[162] Tim Starks, *Trump Administration Ratchets Up Naming and Shaming Nation State Hackers*, POLITICO (June 6, 2018), https://subscriber.politicopro.com/cybersecurity/article/2018/06/trump-administration-ratchets-up-naming-and-shaming-nation-state-hackers-597088.

[163] *See* Timothy Edgar, *A Mini Symposium on Beyond Snowden*, LAWFARE (Sept. 5, 2017), https://www.lawfareblog.com/mini-symposium-beyond-snowden.

[164] *See id.*; *see also* Timothy Edgar, Apple v. FBI *Shows That Lawyers and Tech Speak Different Language on Privacy*, LAWFARE (Mar. 17, 2016), https://www.lawfareblog.com/apple-v-fbi-shows-lawyers-and-tech-speak-different-language-privacy.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

two minds when it comes to government surveillance.[165] Following the 9/11 terrorist attacks, there was broad support for surveillance programs that could enhance national security and prevent future terrorism within the United States.[166] In response, on October 26, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the Patriot Act.[167] The Patriot Act significantly expanded the United States government's authority to investigate all potential threats, allowing the collection of personal information on the Internet.[168] Additionally, under the Patriot Act, United States agencies could search for information "relating to terrorism" within foreign and domestic databases.[169] Title VII of the Patriot Act also reclassified digital information, entitling key United States government officials access to any information that might "lead to terrorism."[170]

However, the release of the Snowden leaks in 2013 caused public opinion to turn against the government.[171] Also, by 2013 smartphones had become so commonplace that Chief Justice Roberts, writing for the Court, stated it was "no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[172] Adding some lightness to the opinion, Chief Justice Roberts also commented that cell phones were "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an

---

[165] *See, e.g.*, Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; *see* Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RESEARCH CTR. (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/.

[166] Maniam, *supra* note 165.

[167] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107–56, 115 Stat. 272.

[168] *See* Dara Lind, *Everyone's Heard of the Patriot Act. Here's What it Actually Does*, VOX (June 2, 2015), https://www.vox.com/2015/6/2/8701499/patriot-act-explain.

[169] *Id.*

[170] *Id.*; 115 Stat. at 274–75.

[171] Abigail Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RESEARCH CTR. (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

[172] Riley v. California, 573 U.S. 373, 395 (2014).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

important feature of human anatomy."[173] Thus, it was perhaps not surprising that the United States government's scope of surveillance displeased many Americans,[174] nor that much of the public discussion continues to focus on government surveillance today.[175]

The private sector plays into the government surveillance narrative by characterizing itself as standing between individuals and the government.[176] One way this has occurred is by embracing encryption and resisting government requests for encryption keys and access to encrypted personal data.[177] This shift has created tension with law enforcement agencies who see the ability to access evidence of potential criminal activity, track the behavior of investigation targets, and protect United States' interests as critical to their mission.[178] Private sector advocates such as Alex Stamos, security chief at Facebook, counter that collaborating with law enforcement by creating back door access or providing encryption keys would be "akin to 'drilling a hole in a windshield.' The entire structure would be so weakened . . . that it would destroy the concept of secure communications."[179] The debate between privacy and security advocates will likely remain a major part of the conversation for the foreseeable future as indicated by the Supreme Court's ruling last term in *Carpenter v. United States*, which held the government's interest in law

[173] *Id.* at 385.

[174] Charlie Savage, *Changes to Surveillance Bill Stoke Anger*, N.Y. TIMES (May 20, 2014), https://www.nytimes.com/2014/05/21/us/politics/changes-to-surveillance-bill-stoke-anger.html?login=email&auth=login-email; *see* Geiger, *supra* note 171.

[175] Ellen Nakashima, *Civil Liberties Groups Urge Judiciary Committee to Press NSA on Surveillance Programs*, WASH. POST (Mar. 18, 2019), https://www.washingtonpost.com/world/national-security/civil-liberties-groups-urge-judiciary-committee-to-press-nsa-on-surveillance-programs/2019/03/18/fe883a56-491d-11e9-93d0-64dbcf38ba41_story.html?utm_term=.39b1ebf4f64a.

[176] *See Chapter One Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance*, 131 HARV. L. REV. 1722, 1726–27 (2018).

[177] *See, e.g.*, Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ (opposing the FBI's request to access the iPhone data of individuals involved in the San Bernardino terrorist attack).

[178] Sheldon Whitehouse, *Why Americans Hate Government Surveillance but Tolerate Corporate Data Aggregators*, LAWFARE (June 2, 2015), https://www.lawfareblog.com/why-americans-hate-government-surveillance-tolerate-corporate-data-aggregators.

[179] SANGER, *supra* note 103, at 249.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

enforcement did not merit "unrestricted access to a wireless carrier's database of physical location information."[180]

Although this Note does not address the United States government's data security practices, they have significant room for improvement. For example, China's 2015 data breach of the Office of Personnel Management ("OPM") highlights the danger that suboptimal data and security architecture poses to both the United States and specific individuals.[181] The breach led the United States to recall numerous diplomatic envoys and intelligence officials from China and exposed the highly personal information of over 22 million individuals.[182] Unfortunately, improving the United States government's entire data architecture is no small task given its vast scope, not to mention the vulnerabilities that state and local governments face.

The convergence of the OPM and the Marriott-Starwood data breaches help explain why the data security practices of private corporations cannot be divorced from United States' national security and foreign policy interests. The 2015 OPM data breach involved highly sensitive personal information including over 4 million people who worked for the federal government at the time.[183] The stolen data included birth dates, Social Security numbers, medical histories, bank information, and detailed background research on applicants for security clearances.[184] The damage to foreign policy and intelligence was immediately apparent and the United States Department of State reacted by pulling certain diplomats from China.[185]

The Marriot-Starwood hack, which involved the information of some 500 million guests, started around the same time period as the OPM hack and continued

---

[180] Adam Liptak, *In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy*, N.Y. TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html.

[181] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[182] Ellen Nakashima, *CIA Pulls Officers from Beijing After Breach of Federal Personnel Records*, WASH. POST (Sept. 29, 2015), https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html?utm_term=.3b09ce57ae85.

[183] Nakashima, *supra* note 175.

[184] *Id.*

[185] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

through 2018.[186] "The names, addresses, phone numbers, birth dates, email addresses and encrypted credit card details of hotel customers were stolen. The travel histories and passport numbers of a smaller group of guests were also taken."[187] Like the OPM hack, the Marriott-Starwood breach has also been attributed to state-sponsored Chinese actors.[188] The information from these two hacks alone—which are just some of the many hacks in the past decade and involve only one United States geopolitical rival or adversary—could be used "to identify or recruit an American intelligence agent, nuclear weapons engineer or vulnerable diplomat."[189] Moreover, the lines between the federal government, the government contractors, the military establishment, and the private sector are thin, and security risks could easily travel with an individual from role to role.[190]

Accepting that cyber is here to stay and acting accordingly is a requirement for any modern global power. More generally for nation-states, the geopolitical implications of cyber threats represent a new frontier full of pitfalls. Henry Kissinger, writing in *Nuclear Weapons and Foreign Policy*, identified from the outset that nuclear weapons would transform geopolitics, and that such "[a] revolution cannot be mastered until it is understood."[191] Modern geopolitics grew out of the emergence of nation-states roughly 200 years ago.[192] Specifically defined borders that mark where one nation's sovereignty starts and another nation's sovereignty stops are one of the hallmarks of the nation-state. The flattening of the world by the Internet has arguably turned the geopolitical framework on its head. A country's borders can no longer be defined by physical barriers such as coastlines, rivers, and mountains that can be protected by border guards and armies. The interconnected cyber world that exists today allows for threats to originate or be masked as coming from thousands

[186] Nicole Perlroth et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

[187] *Id.*

[188] Christopher Bing, *Exclusive: Clues in Marriott Hack Implicate China—Sources*, REUTERS (Dec. 5, 2018), https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D.

[189] David Sanger et al., *Attack Gave Chinese Hackers Privileged Access to U.S. Systems*, N.Y. TIMES (June 20, 2015), https://www.nytimes.com/2015/06/21/us/attack-gave-chinese-hackers-privileged-access-to-us-systems.html.

[190] *See* Brian Wallheimer, *Should We Stop the 'Revolving Door'?*, CHI. BOOTH REV. (Aug. 7, 2017).

[191] SANGER, *supra* note 103, at xxi.

[192] *See generally* Andreas Wimmer & Yuval Feinstein, *The Rise of the Nation-State Across the World, 1816 to 2001*, 75 AM. SOC. REV. 764 (2010).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

of miles away. Understanding the implications of cyber power, threats, and weapons on strategic decisions and geopolitics generally may well require a wholesale government reorganization of resources and assumptions.

Regulation could help address the vulnerabilities that uncertain private sector data privacy and cyber security standards have created for the United States' interests. Currently, there are essentially fifty different data privacy regulatory schemes for fifty different states.[193] Without a cohesive federal approach to data privacy, the United States' cyber strategy amounts to thousands of individual soldiers defending themselves separately against coordinated attacks by modern armies. Implementing federal regulations that govern how private companies deal with the private data of their customers could lead to improved data security practices. In addition, companies faced with fines and reporting requirements would have every incentive to cooperate with the United States government to prosecute wrongdoers, and put in place measures that avoid hacks and data breaches in the first place.

However, attempting to legislate corporations' regulation of data privacy in the name of the best interests of United States' national security goals might ultimately be a fool's errand. One challenge for any proposed regulatory scheme involving technology is that the speed of innovation in the technology sector can make a proposed bill or regulation outdated by the time it clears Congress or the agency.[194] The cyber world, however, moves quickly.[195] A recent display of the challenge posed by the slow pace of regulation is the post-2000 presidential election effort to implement electronic voting.[196] Well-intentioned, electronic voting machines have created major vulnerabilities in voting systems around the country.[197] Now, even in the face of overwhelming evidence of election systems' vulnerabilities, Congress has

[193] *See* David Lohrmann, *New Guide on State Data Breach Laws*, GOV'T TECH. (Sept. 1, 2018), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-guide-on-state-data-breach-laws.html.

[194] Mark D. Fenwick et al., *Regulation Tomorrow: What Happens When Technology Is Faster Than the Law?*, 6 AM. U. BUS. L. REV. 561 (2017).

[195] Drew DeSilver, *Chart of the Week: The Ever-Accelerating Rate of Technology Adoption*, PEW RESEARCH CTR. (Mar. 14, 2014), https://www.pewresearch.org/fact-tank/2014/03/14/chart-of-the-week-the-ever-accelerating-rate-of-technology-adoption/.

[196] *See* Kim Getter, *The Crisis of Election Security: As the Midterms Approach, America's Electronic Voting Systems Are More Vulnerable Than Ever. Why Isn't Anyone Trying to Fix Them?*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

[197] *See id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

been unable to act.[198] Thus, any solution, however well-intentioned, should be flexible and adaptable to emerging technologies and threats.

Technology companies, however, are not waiting for nations to establish international norms on the use of cyber force and are looking to shape the conversation through efforts such as the "Digital Geneva Convention" or "Cyber Tech Accord."[199] Proposed by Microsoft President and Chief Legal Officer Brad Smith, the accord is a private sector plan to institute global rules that protect the civilian use of the Internet.[200] Led by Microsoft and Facebook, the proposal was signed by thirty-four companies in March 2018 and has grown to over sixty companies.[201] Although not binding, the Convention commits signors to "not help any government—including that of the United States—mount cyberattacks against 'innocent civilians and enterprises from anywhere.'"[202] The companies also commit to "come to the aid of any nation on the receiving end of such attacks, whether the motive for the attack is 'criminal or geopolitical.'"[203] However, by focusing on "protecting users and customers everywhere," the accord creates an inherent tension with the interests of nation-states bound to serve a specific geography and population group.[204]

Regulating the data privacy and security practices of companies operating within the United States would create unavoidable costs for companies to comply with its regulations and respond to assertions of individual rights concerning data.[205]

---

[198] *See id.* Such is the reality in Congress today, where the current dearth of bipartisan collaboration in the United States Congress has stalled innovative proposals from both sides of the aisle. Derek Willis & Paul Kane, *How Congress Stopped Working*, PROPUBLICA (Nov. 5, 2018), https://www.propublica.org/article/how-congress-stopped-working.

[199] *Cybersecurity Tech Accord*, TECH ACCORD, https://cybertechaccord.org/accord/ (last visited Oct. 2, 2019).

[200] *A Digital Geneva Convention to Protect Cyberspace: Microsoft Policy Papers*, MICROSOFT, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH (last visited Oct. 2, 2019).

[201] Michael J. Miller, *Microsoft President Calls for Digital Geneva Convention to Fight Cyber Attacks*, PC MAG. (Oct. 2, 2018), https://www.pcmag.com/article/364123/microsoft-president-calls-for-digital-geneva-convention-to.

[202] David E. Sanger, *Tech Firms Sign Digital Geneva Accord Not to Aid Governments in Cyberwar*, N.Y. TIMES (Apr. 17, 2018), https://www.nytimes.com/2018/04/17/us/politics/tech-companies-cybersecurity-accord.html.

[203] *Id.*

[204] *See A Digital Geneva Convention to Protect Cyberspace: Microsoft Policy Paper*, *supra* note 200.

[205] *See* Frenkel, *supra* note 82.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu

However, it also may shine the light on unknown data collection and processing practices—which may well be externalizing costs and harm to customers.[206] If the GDPR proves effective at curtailing negative practices without creating too great a chill on innovation, similar regulations may soon migrate to the United States and other countries, regardless, due to consumer pressure.

Ultimately, upholding America's position may require a transformative approach to education, intelligence, military, and the economy—that is to say, to every aspect of modern society. An incremental or linear approach to meeting cyber threats could merely ignore the lessons of history and doom them to repetition. "We keep digging for new technological solutions—bigger firewalls, better passwords, better detection systems—to build the equivalent of France's Maginot Line. Adversaries do what Germany did: they keep finding ways around the wall."[207]

Cyberattacks are not going anywhere. It may well be impossible to maintain completely the United States' past position of power in the cyber sphere, but inaction is not a choice in a rapidly developing arena. Therefore, it is time for the United States to comprehensively reassess its approach to cyber power and regulating data privacy could be a significant step towards effectively protecting and advancing the nation's interests on the global stage.

[206] Calo & Rosenblat, *supra* note 35, at 1655, 1669 (footnotes omitted).

[207] SANGER, *supra* note 103, at xxii.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2019.681
http://lawreview.law.pitt.edu