Loyola University Chicago International Law Review

Volume 15 | Issue 2 Article 4

2018

Failed Herd Immunity: American Business Compliance and the United States Cyber-Security Policy's Clash with the European Union's General Data Protection Act

William Dimas

FAILED HERD IMMUNITY: AMERICAN BUSINESS COMPLIANCE AND THE UNITED STATES CYBER-SECURITY POLICY'S CLASH WITH THE EUROPEAN UNION'S GENERAL DATA PROTECTION ACT

William Dimas*

I. Introduction

In biology, the concept of herd immunity refers to the process of protecting a whole group from a disease by immunizing a critical mass of its populace.[1] Once that critical mass is immune, the likelihood of outbreak is reduce significantly, leading to the longevity of the group.[2] The herd immunity model goes beyond animals, however, and can be applied to the future of personal data security around the world. On May 25, 2018, the European Union will enforce its new data protection laws, the General Data Protection Regulation (GDPR).[3] All foreign companies and organizations that operate within the European Union or with data processing outside of the EU will need to comply with the GDPR if they wish to carry on their business and store and process European data.[4] With their requirements of compliance, the EU is exporting their data privacy values abroad and setting a standard for the international community to establish for their own citizens, offering the world a privacy vaccination. While a step towards future rights for the international community, it is more likely that organizations will create two-tiers of data protection systems in order to comply with the new regulations and continue to maintain many of their data processing and selling

* JD Candidate, Loyola University Chicago School of Law.

[1] Emily Willingham & Laura Helft, *What is Herd Immunity?* NOVA, http://www.pbs.org/wgbh/nova/body/herd-immunity.html.

[2] *Id.*

[3] Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Apr. 19, 2018), http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[4] Burgess, *supra* note 3.

practices. These data values will have a minimal effect on influencing data protection policy for U.S. citizens. Through continued massive surveillance and the intent of passing the FISA Amendments Act of 2017 (H.R. 4478) in an effort to renew and expand the Executive branch's power over data collection and surveillance under Section 702, the Executive branch seeks to circumvent the GDPR rights and private sector compliance. While the GDPR will likely mitigate some of the average consumer threats from external forces and sale of information from private businesses, the expansion of H.R. 4478 and the temporary ban on "about target" searches will override the protections that the EU has afford to its citizens, negating the vaccination attempts by the EU. In other words, the critical mass will not be reached.

The background is split into two parts. The first section will focus on the history of data protection in Europe, the problems that led to the replacement of the previous legislation called the Data Protection Directive 95/46/EC (DPD), and the contents of the GDPR. This will include the goals of the new legislation and the rights that have been carved out for EU citizens.

The second section will analyze the cyber-threats that currently faced by the American public and the international community and the ineffectual options for retaliation or prevention of cyber-attacks. This will establish why providing citizens with the opportunity to protect their own information through various rights is a security bonus.

Delving into the history of Foreign Intelligence Surveillance Act (FISA), this article will assess the scope of current U.S. cyber security programs and regulatory agencies under Foreign Intelligence Surveillance Act (FISA) Amendments of 2008, and the new amendments to FISA under H.R. 4478 upon these agencies.

The analysis will focus on the theory of herd immunity and how U.S. businesses and organizations will integrate the compliance requirements of the GDPR when processing European data, while still providing massive amounts of data to national security agencies allowed under the exceptions to these rights for surveillance and under the expansion of FISA Amendments Act of 2008 through the H.R. 4478. As total compliance is an the unreasonable expectation and the creation of a two-tiered system of data protection will ultimately leave international and European data at greater risk from the cyber-security threats and government overreaching. In Part 2, the discussion will turn to preventing either group from being protected preventing either group from being protected and simultaneously allowing a potential FISA renewal to circumvent the rights completely.

Finally, the proposal will discuss the need for a restriction on FISA and a change in the American view of the commodity of data in order to ensure the effectiveness of the GDPR. Without this change, the GDPR, while effective in the short-term, will not be an international change, despite being the premiere protection of consumer data rights.

II. Background

A. European Data Protection History and the GDPR

Citizens of EU member states are protected under a stronger and more holistic framework than the United States has because the EU has a recognized right to data privacy.[5] Europe's strong history of data protection extends back to the early days of the UN.[6] In the aftermath of World War II and at the beginning of the Cold War, the UN recognized how the collection and storage of civilians' personal information allowed governments, like the Nazis, to target individuals and groups during purges.[7] This gruesome realization influenced the European Convention on Human Rights to include protections of data, basing European's rights on dignity and honor.[8] While some European nations established their own data protection acts in the late 1970s, the UN began drafting guidelines to govern data for other states to adopt.[9] The process was slow and arduous, but ultimately finalized a decade later.[10]

Fifteen years later, in October 1995, the DPD was passed and became the guiding principles for adjudicators in the EU data protection realm for the next twenty years.[11] The DPD were based on the Fair Information Principles, providing rights to information, access to the data, and the ability to rectify the data, if necessary.[12] These rights were a minimum standard for national law and the various member states could add more additional protection laws, depending on what they believed was necessary.[13] Paired with these rights, the DPD employed an adequacy requirement, requesting that Member States deal exclusively with third parties, further requiring countries to provide adequate protection for data.[14]

---

[5] Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111, 1114 (2018) [hereinafter Watanabe].

[6] Steven S. Mccarty-Snead & Anne Titus Htlby, *Research Guide to European Data Protection Law*, 42 INT'L J. LEGAL INFO. 348, 360 (2014).

[7] *Id.*; *see also* Charles Hawley, *Fifty Million Nazi Documents: Germany Agrees to Open Holocaust Archive*, SPIEGEL ONLINE (Apr. 19, 2006), http://www.spiegel.de/international/fifty-million-nazi-documents-germany-agrees-to-open-holocaust-archive-a-411983.html (30-50 million documents detailing the exterminations within the camps in clear detail, the sheer volume of information reinforces the dangers that can occur when personal data is abusively collected).

[8] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 967 (2016) [hereinafter McGeveran].

[9] Paul de Hert & Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?* 9 I/S: J. L. POL'Y INFO. SOC'Y 271, 281-82 (2013) (France and Germany had already implemented data protection policies, with the French Law on Informatics, Data Banks and Freedoms (1978) and the first Federal Data Protection Act (1977)).

[10] *Id.* at 282.

[11] Watanabe, *supra* note 5, at 1119.

[12] de Hert & Papakonstantinou, *supra* note 9, at 10.

[13] McGeveran, *supra* note 8, at 969.

[14] The EU-US Privacy Shield Framework is based on this adequacy principle. *See also* de Hert & Papakonstantinou, *supra* note 9, at 279.

By 2012, the DPD was ineffective and unable to cope with modern technological strategies that threaten personal information online.[15] While the DPD was founded on many of the same principles as the GDPR legislation, its minimum requirements led to a lack of standardization throughout EU member states, hindering the data transfer channels between nations.[16] The obligations of companies under the legislation created administrative burdens and excessive costs.[17] The inherent distrust in the data protection abilities between member states threatened potential economic stagnation, as the benefits of trading and operating within a member state with weaker data protection laws exposed the information to a variety of cyber-threats and thefts. The U.S. National Security Agency (NSA) further exacerbated the fears of intrusions into EU data privacy when Snowden leaked information revealing the NSA systematic and chronic data collection and storage practices, without the employment of proper oversight and respect for the privacy rights under the DPD.[18] After four years drafting and revisions, the GDPR was approved in 2016, with an enforcement date of May 25, 2018.

Replacing the DPD and drawing upon Article 8(1) of the Charter of Fundamental Rights of the European Union, the GDPR posits that every European citizen has a right to protection of personal data. The intention behind this right is to encourage freedom, increase security, and support justice.[19] In addition to the protections, the GDPR seeks to strengthen the economics of the EU and harmonize the cyber-laws to encourage trust and growth.[20]

Article 5 of the GDPR sets forth the principles and limitations for organizations that fall under its jurisdiction.[21] The data must be lawfully and fairly processed, in a transparent manner and for an explicitly, specified purpose. To accomplish this, the GDPR will include restrictions on the length of time that

---

[15] *GDPR Timeline of Events*, EUGDPR.ORG, https://www.eugdpr.org/gdpr-timeline.html; de Hert & Papakonstantinou, *supra* note 9, at 311 (frameworks for new data protection acts were reviewed starting in 2009, but the first drafts of the what would become the GDPR were presented in 2012).

[16] General Data Protection Regulation, COUNCIL OF THE EUROPEAN UNION (Apr. 6, 2016) at art. 9, http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf [hereinafter GDPR]; *see also* Scott J. Shackleford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Study*, 67 S.C. L. REV. 609 (Spring 2016) (the continuous struggle of centralization, in which EU member states seek to maintain their sovereignty and individual national goals, while simultaneously seeking to create more accountability and smoother operations complicates the future of cybersecurity policy despite the newest legislation).

[17] Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight-What Proposed EU Data Regulation Means For U.S. Companies*, 28 SANTA CLARA HIGH TECH. L.J. 815, 817-18 (2012).

[18] Ewen Macaskill & Gabriel Dance, *NSA Files Decoded*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

[19] GDPR, *supra* note 16, at preamble; Rohan Massey, Heather Sussman, et al., *Countdown to Compliance: One Year to go until GDPR Enforcement*, ROPES & GRAY 1, 2 (May 26, 2017) [hereinafter *Countdown to GDPR Compliance*].

[20] GDPR, *supra* note 16; *Countdown to GDPR Compliance*, supra note 19.

[21] GDPR, *supra* note 16, at art. 5.

data may be held and for long that data may be used to identify the citizen.[22] This Fair Processing Principle will carry over from the DPD, relating to collection, disclosure, retention, and disposal of personal data.[23]

The GDPR will continue to guard European citizens' rights regarding the ability to access their own personal data. It will also impart a right to erasure; a right to rectification; new rules regarding consent; data portability rights; a right to be informed; a right to object; and rights related to automated decision making including profiling.[24]

The right for a citizen to be informed is guaranteed under Articles 13-15 of the GDPR.[25] When collecting and processing data, a data controller must inform citizens as to the purpose of the collection of data the recipient of the data, and the time frame for the collection of the data.[26] If a data controller has received personal data from another source, the controller must state where the information originated, the legal basis for that information, other recipients of that information, and the categorization of data received.[27] Article 15, known as the right of access, allows the citizen to request and obtain a confirmation from the data controller as to whether the personal data is being used and the reason for its use. Further, as an additional safeguard, when information is transported outside of this country, the data controller must list the protective measures utilized by the recipient country to protect personal data.[28]

Under the right to erasure, commonly dubbed "the right to be forgotten" in the U.S., individuals may request the removal of processed personal data if: (1) the data is no longer a necessity; (2) has no relation to the original purpose; (3) the individual has withdrawn consent; (4) the data was unlawfully processed under the GDPR; (5) the data must be deleted for compliance; or the data references a minor.[29] The right to erasure also existed under the DPD and was most notably applied in a case from the Court of Justice of the European (CJEU), in which Google Spain was ordered to honor requests to remove unnecessary data.[30] The court cited the economic incentives to remove out-of-date information as a boon to Google. Following the establishment of a request mechanism to have data

---

[22] *Id.*

[23] Processing Personal Data Fairly and Lawfully (Principle 1): What Does Fair Processing Mean? INFORMATION COMMISSIONER'S OFFICE (last visited on Dec. 4, 2017) https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/.

[24] GDPR, *supra* note 16; *Countdown to GDPR Compliance*, supra note 19, at 2; Watanabe, *supra* note 5, at 1120-21.

[25] GDPR, *supra* note 16, at arts. 13-15; *$51.04 The General Data Protection Act*, 6-51 COMPUTER L. 1, 5-7(2016) [hereinafter *$51.04 GDPR*].

[26] *Id.* at 5-6 (Article 13).

[27] *Id.* at 6 (Article 14).

[28] *Id.* at 6-7.

[29] GDPR, *supra* note 16, at art. 17; Right to Erasure, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (last visited Dec. 3, 2017).

[30] *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.J. C-131/12, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN.

removed, Google reported receiving hundreds of thousands of requests for data to be removed from every EU member state.[31]

In conjunction with the right of erasure, Article 7 requires conditional consent dependent on the processing of particular data.[32] Data controllers must ensure that the consent that they have received is specific to the purpose under which they are processing the data. Citizens are allowed to freely give and revoke consent in relation to the processing of their data.[33] Article 9 of the GDPR provides a list of personal data types, ranging from racial origins to political affiliations to sexual orientation, which may never be processed except for circumstances with explicit consent or the use in defense of legal claims.[34]

Known as the right of portability, Article 20 of the GDPR allows citizens the right to receive the data from the data controller in a form that the citizen may employ for personal use.[35] The data controllers must provide two types of data to the citizen upon request: (1) data actively and knowingly provided and (2) data observed via use of the service of a device.[36] Data controllers are required to maintain the minimum amount of information for the limited duration that a citizen uses the service provided. Third parties are only allowed to see the maximum amount of information they need to accomplish their action, rather than having access to an entire individual's metadata on the app.[37]

Article 3 of the GDPR expands the territorial scope of the individuals and organizations that must comply with the legislation under the new law.[38] To overcome the previous ambiguity of whether the Directive applied, the GDPR is explicit and states that all data controllers and data processors that work with EU data will be responsible for complying, regardless of their place of business. Furthermore, all non-EU business will have to select an EU representative if they process the data of EU citizens.[39] This includes organizations that provide free goods and services to customers in the European markets.[40] EU states are responsible for ensure that their laws comply with the GDPR.

---

[31] W. Gregory Voss & Celine Castets-Renard, *International and Comparative Technology Law: Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A study on the Convergence of Norms*, 14 COLO. TECH. L.J. 281, 287 (2016) (519,733 search engine results, as of April 2, 2016, indicate the right is widely exercised in the EU).

[32] *§ 51.04 GDPR*, *supra* note 25, at 4.

[33] *Id.*

[34] *Id.*

[35] *Id.* at 32-33.

[36] *Id.* at 33 (The GDPR does not require data that has been inferred based off the other forms be provided to the data subject).

[37] *Id.*

[38] Linda V. Priebe, *How EU Data Privacy Reform Will Impact US Telecom Cos.*, LAW360 (Mar. 21, 2017), https://www.law360.com/articles/903685/how-eu-data-privacy-reform-will-impact-us-telecom-cos-.

[39] GDPR Key Changes, https://www.eugdpr.org/.

[40] AJ Dellinger, *EU's GDPR: What Will American Companies Have to Do to Comply*, INT'L BUS. TIMES (Aug. 1, 2017), http://www.ibtimes.com/eus-gdpr-what-will-american-companies-have-do-comply-2573002.

Data controllers and data processors will also have heightened responsibilities related to security, requiring that the implementation of security measures be proportionate and appropriate for the risks that are present, rather than simply having an arbitrary level of security.[41] The previous requirements on alerting the affected parties of security breaches without undue delay for telecommunication companies under the Directive will be expanded under the GDPR to include all companies.[42] In the event of a breach that impacts personal data, entities will be required to report that breach within 72 hours.[43]

To regulate compliance, the GDPR establishes a European Data Protection Board (EDPB) to guide the formation of compliance. EDPB will approve code practices and certification schemes for various entities. As an appellate body, the EDPB reviews disputes that will inevitably arise.[44] Failure to comply with the new regulations or infringing on a person's rights will result in a fine of either 4% or 20 million pounds, whichever amount is larger.[45]

These rights are not absolute rights under Article 23 and Chapter IX of the GDPR and will be subjected to a variety of limitations, such as for the national defense, persecution of a crime.[46] Under a necessary and proportionate standard of review, member states are allowed to introduce exemptions and derogations that would further allow the processing of data beyond the limits set for in Article 5.[47]

B. Cyber Threats and the New Battlefield

In 2014, the United States charged five Chinese military hackers with computer hacking, economic espionage and other offenses directed at targets within various United States industries, ranging from nuclear power to the metals products industry.[48] After assessing the theft, this event was described as one of the greatest exchanges of economic wealth in history by U.S. officials. The threat of cybercrime has continued to rise and became the second most reported economic crime affecting organizations in 2016.[49] Many companies were not equipped to deal with attacks. Less than 37% of the affected companies had cyber security

---

[41] Michael Drury & Julian Hayes, *England & Wales,* CYBERSECURITY 28, 30 (Benjamin A. Powell & Jason C. Chipman ed., 2018); Gilbert, *supra* note 17, at 819.

[42] *Id.*

[43] Shannon Yavorsky, GDPR- Unlocking the Security Obligations, LAW360 (July, 20, 2017).

[44] Drury & Hayes, *supra* note 41, at 819.

[45] *Id.*

[46] *Id.*

[47] *Exemptions*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/exemptions/ (last visited on Apr. 12, 2018).

[48] Press Release, U.S. DEP'T OF JUSTICE, U.S. CHARGES FIVE CHINESE MILITARY HACKERS FOR CYBER ESPIONAGE AGAINST U.S. CORPORATIONS AND A LABOR ORGANIZATION FOR COMMERCIAL ADVANTAGE (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[49] *Global Economic Crime Survey 2016:Adjusting the Lens on Economic Crime: Preparation Brings Opportunity Back Into Focus*, PwC (2016) https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf.

plans in the event of a cyber hack.[50] These hacks have left hundreds of millions of Americans exposed to identity theft and reveals major flaws in the handling of American data and the lack of defense mechanisms.[51] In a world where the battlefields have morphed, civilians and civilian infrastructure have become prime and poorly defended targets besieged by unceasing cyber-attacks.[52]

As one of the most powerful equalizing strategies, cyber-attacks provided nations who employed cyber tactics the ability to cripple critical infrastructure as a deterrent, collect military secrets, and employ industrial espionage while acquiring a massive economic advantage.[53] Speed and anonymity provide significant advantages to states employing aggressive, offensive cyber strategies against other nations who must sink huge quantities resources for defense.[54] The devastating effects of cyber-attacks can immediately plunge a country into a state of emergency or slowly deplete their technological capabilities and tactics over time.[55] Most attacks are difficult to trace and even harder to identify the perpetrator, leaving no one to hold accountable and allowing for plausible deniability from state actors.

Additionally, the available responses for hacks are limited, as nations often lack the jurisdiction to properly prosecute hackers, especially those operating in foreign countries.[56] Convictions, similar to the ones the five Chinese hackers were handed, are rare. Many believe the best strategy is to establish international guidelines through diplomacy but that has been ineffective. During his tenure as president, President Obama attempted to reach agreements with Chinese President Xi Jinping, but failed to make any major headway before leaving office.[57]

---

[50] *Id.*

[51] Michael Riley, Jordan Robertson, and Anita Sharp, *The Equifax Hack has the Hallmarks of State-Sponsored Pros*, BLOOMBERG BUSINESSWEEK (Sept. 29, 2017) https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [hereinafter *The Equifax Hack*]; Andrew Ubaka Iwobi, *Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime*, 26 TRANSNAT'L L. & CONTEMP. PROBS. 13, 30 (Winter 2016) (discussing Lord Hoffman's analysis in R v. Brown as to the invasive nature of modern technology through data collection and transmission).

[52] *See*, Frédéric Mégret, *War and the Vanishing Battlefield*, 9 LOY. U. CHI. INT'L L. REV. 131 (2011) (discussing the shifts away from traditional confined battlefields and the difficulties this proposes for the enforcement of the laws of war).

[53] Magnus Hjortdal, *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence*, J. OF STRATEGIC SEC. 4, NO. 2, 1 (2011).

[54] *Id.*

[55] Scott J. Shackleford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Study*, 67 S.C. L. REV. 609 (Spring 2016).

[56] Jyh-An Lee, *The Red Storm in Unchartered Waters: China and International Cyber Security*, 82 U. MO.-KAN. CITY L. REV VOL. 82, NO. 4., 951, 959 (2014).

[57] Aamer Madhani, *Obama, Xi get Closer but Gap Remains on Cybersecurity*, USA TODAY (June 8, 2013), https://www.usatoday.com/story/news/politics/2013/06/08/obama-xi-take-stroll/2403823/.

III. Discussion: The Shield and the Net, U.S. Cyber-Security Strategies and Future

While the European Union has chosen to protect those rights, U.S. policy seeks to expand the national security expectations of surveillance to combat the threats above. US privacy law has, by contrast, largely developed in a "patchwork", with an array of state and federal statutes of common law doctrine.[58] At the federal level, the strongest data protection rights come from data protection regimes like the Health Insurance Portability and Accountability Act ("HIPAA") and the Children's Online Privacy Protection Act ("COPPA").[59] In a manner similar to the EU under the DPD, the majority of data protections are provided at an individual state level and these wildly vary from state to state.[60] Due to this lower threshold for privacy and censorship laws, users have different experiences when visiting websites in the United States, as opposed to within the EU.[61]

While the Fourth Amendment of the Constitution provides protection from unreasonable search and seizures from the government, it does not guarantee a right to personal information stored from private actors.[62] Since 9/11, many of the original protections for U.S. citizens regarding their data have been eroded, including the protections provided by the Foreign Intelligence Service Act of 1978 (FISA 1978). FISA 1978 was originally drafted with a dual purpose in mind. In the wake of the Watergate Scandal, it was discovered that CIA operatives had conducted missions on domestic soil, breaking their mandate.[63] The CIA infiltrated political activist groups, unions and other elements of domestic society, as they believed these groups were working with foreign dissidents and spies to disrupt national security.[64] Thus, FISA 1978 was written to operate as both a limit on the surveillance powers of the Executive branch and as a framework to conduct international intelligence gathering and countermeasures, including instances when the data of U.S. citizens are involved.[65] Under the minimization principle, analysts are and are still required to reduce the effect and intrusions on the rights of Americans when collecting data investigating foreign intelligence and nationals.[66]

---

58 McGeveran, *supra* note 8, at 965.

59 *Id.*

60 *See*, Watanabe, *supra* note 5, at 1122 (the state that provides the strongest protections, California, has its own version of the right of erasure exclusively for minors).

61 Victor Luckerson, *Americans Will Never Have the Right to be Forgotten*, TIME (May 14, 2014), http://time.com/98554/right-to-be-forgotten.

62 U.S. CONST. amend. IV; Sherri J. Deckelboim, Note, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework Will Impact Advocates, National Security, And Businesses*, 48 GEO. J. INT'L L. 263, 272 (2016).

63 The Foreign Intelligence Surveillance Act of 1978, DEP'T OF JUSTICE, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286 [hereinafter FISA 1978 Overview Page].

64 *Id.*

65 FISA 1978 Overview Page, *supra* note 63; United States v. Rosen, 447 F. Supp. 2d 538, 542 (E.D. Va. 2006). *See also*, Macaskill & Dance, *supra* note 18, at 3.

66 FISA 1978 Overview Page, *supra* note 63.

Starting in 1995, FISA 1978 has been revised and amended seven times, the most notable being the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act and the FISA 2008 Amendments Act of 2008 (FISA 2008).[67] In 2008, the FISA regulation was updated to include Section 702, which provided the authority for security agencies to compel telecommunication networks to aid in the acquisition of foreign intelligence information related to non-US persons residing in foreign countries.[68] The framework followed shares some similarities with FISA 1978. To request information, analysts must show that they have properly determined the location to be outside of the U.S. and have taken steps to minimize and remove the domestic communications.[69] Any data collected that still includes a U.S. citizen and a foreign national target is permissible so long as the intrusion into the data of American citizens is minimized. Analysts compile this information into a certification, in lieu of a search warrant, showing that the proper collection procedures were followed.[70] An annual review process is used to ensure protocols are up-date and followed.[71]

Under Section 702, the NSA describes data collections as "upstream" and "downstream" collection.[72] Within Upstream collection, the NSA intercepts data over fiber cables and from infrastructure. The NSA collects data and communications throughout the world, most of which goes through the United Kingdom and the United States.[73] The NSA defines "upstream" data collection as "[collections acquired from] communications 'to, from, or about' a Section 702 Selector".[74] Of the two collection methods, "upstream" accounts for smaller accounts, with some estimates sitting at 9% of the total data collection.[75] The "about target" data is information that is communicated between individuals, who are not targets themselves, about a topic or discussion that is a target in question.[76] This allows the NSA to collect information from anyone, including two parties of American citizens, so long as the NSA identifies a specific target and relation to the threat

---

67 *Id.*

68 FISA Amendments Act of 2008 Section 702 Summary Document, OFFICE OF GENERAL COUNSEL 1, 3 (Dec. 23, 2008).

69 Upstream v. PRISM, ELEC. FRONTIER FOUND, https://www.eff.org/pages/upstream-prism (last visited Dec. 4, 2017).

70 *Id.* at 6-12.

71 Ellen Nakashima, *NSA Halts Controversial Email Collection Practice to Preserve Larger Surveillance Program*, WASH. POST (Apr. 28, 2017) https://www.washingtonpost.com/world/national-security/nsa-0halts-controversial-email-collection-practice-to-preserve-larger-surveillance-program/2017/04/28/e2ddf9a0-2c3f-11e7-be51-b3fc6ff7faee_story.html?utm_term=.31e7ae911c71.

72 Public Statement, NSA Stops Certain Section 702 "Upstream" Activities, NAT'L SEC. AGENCY (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml [hereinafter Public Statement].

73 Macaskill & Dance, *supra* note 18, at 3 (the NSA nicknamed the flow of data 'home field advantage' due to the high amounts that travel through allied territory).

74 Public Statement, *supra* note 72.

75 Nakashima, *supra* note 71.

76 Public Statement, *supra* note 72.

being investigated.[77] This is a circumvention to the minimization principle set forth in the original FISA.[78] Following serious missteps and abuses of civil liberties and the potential repeal of Section 702 as whole and cease spying in court, NSA offered to regulate themselves and voluntarily cease the "about target" searches.[79] The removal allowed Section 702 surveillance to continue collecting large quantities of data "upstream", only when the communications were between foreign nationals.[80]

In tandem with the upstream collection operations, PRISM is the downstream data collection counterpart responsible for collecting data from major US Internet companies.[81] Defined as "[the collection of] communications 'to or from' a Section 702 selector", Prism collected data, such as search history and emails, directly from participating business' servers, beginning with Microsoft on September 11, 2007.[82] Prior to the Snowden's document lease, major businesses were complying with security requests for data were releasing up to 20,000 customer accounts per year and it frequently data collected from Prism usually appeared in the President's daily intelligence report.[83] Many of the companies that were provided data through PRISM later denied knowledge when the existence of the program was revealed.[84]

In response to the Snowden revelations, an Austrian student and Facebook user, Max Schrems, learned that his data was being collected by Facebook's subsidiary in Ireland and transferring it to the United States improperly.[85] Bringing his claim to the Irish Data Protection Commissioner, the initial case was thrown out because the US was deemed to ensure 'adequate' levels of protection under the Safe Harbor framework.[86] Schrems appealed to the High Court of Ireland and the case was placed in the Court of Justice of the European Union (CJEU).[87] The Advocate General of the EU, Yves Bot, described the Safe Harbor as a compromised framework that acted as a conduit for the US data collection programs under the NSA, rather than as a recourse mechanism for EU citizens.[88] As a

---

77 Nakashima, *supra* note 71.

78 *Id*; Michelle Richardson, *Time to Permanently End NSA's "About" Searches in Communications Content under FISA 702*, CENTER FOR DEMOCRACY & TECHNOLOGY, (Jun. 22, 2017) https://cdt.org/blog/time-to-permanently-end-nsas-about-searches-in-communications-content-under-fisa-702/.

79 Nakashima, *supra* note 71.

80 Public Statement, *supra* note 72.

81 Macaskill & Dance, *supra* note 18, at 3; *See also*, Nakashima, *supra* note 71.

82 Macaskill & Dance, *supra* note 18, at 3 (the PRISM slides were leaked by Edward Snowden in 2013).

83 Mark Prigg, *Technology Giants Reveal How Often They are Ordered to Turn Over Information to the Government (and it's Thousands of Times a Month)*, DAILY MAIL (Feb. 3, 2014), http://www.dailymail.co.uk/sciencetech/article-2551277/Technology-giants-reveal-ordered-turn-information-Government.html; Nakashima, *supra* note 71.

84 Macaskill & Dance, *supra* note 18, at 3.

85 Schrems v. Data Protection Commissioner, ELECTRONIC PRIVACY INFORMATION CENTER (last visited Apr. 2, 2018), https://epic.org/privacy/intl/schrems/ [hereinafter EPIC Schrems].

86 EPIC Schrems, *supra* note 85.

87 *Id.*

88 *Id.*

guaranteed right under the EU charter, the failure to provide adequate recourse made the Safe Harbor framework inoperable.[89] The CJEU agreed and ruled that the Safe Harbor framework did not ensure the adequacy threshold due to the intrusive nature of the American data collection system for Schrems.[90]

Due to a combination of mistrust of U.S. data collection and massive surveillance, coupled with serious, external cyber-threats, a framework was established to enable the secure international transfer across the Atlantic. While the EU and U.S. were renegotiating the Safe Harbor framework prior to the Schrems decision, the invalidation disrupted the flow of transatlantic data.[91] Known as the EU-US Privacy Shield, the U.S. Department of Commerce and European Commission established a voluntary method for companies to implement protections and receive approval to meet adequacy standards under the DPD.[92] To overcome the past problems with the DPD, the Privacy Shield framework allows businesses certify that they reach adequate levels of data protection and allows European business to know who allows their citizens recourse.[93] Its goals are to support the transatlantic transfer of data and imbue more trust into the system of data protection.[94] The U.S. government has done little to reinforce European trust in such frameworks.[95]

To further complicate the diplomatic situation, H.R. 4478 was passed and signed, renewing and amending Section 702 and FISA 2008 on January 19, 2018.[96] Controversy surrounded the amendment of FISA 2008 in late November, 2017, as it provided lawmakers with less than 48 hours to make decisions regard-

---

[89] Case C-362/14, Maximillian Schrems v Data Protection Comm'n, Opinion of the Advocate General Bot (Sept. 23, 2015), ¶218, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd4c797cdcac6340d7a77ba9c727a1d350.e34KaxiLc3qMb40Rch0SaxuRaN90?text=&docid=168421&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=524326 ("[. . .owing to the breaches of fundamental rights described above, the safe harbor scheme which it establishes cannot be regarded as ensuring an adequate level protection of the personal data transferred").

[90] EPIC Schrems, *supra* note 85. Schrems has filed a second trial, denoted colloquially as *Schrems II*, that focuses on the validity of standard contractual clauses and whether the transfers under this method in fact adequate. Adam Finlay & Paul Lavery, Validity of Standard Contractual Clauses to be referred to CJEU, McCann FitzGerald (Oct. 4, 2017) https://www.mccannfitzgerald.com/knowledge/privacy/validity-of-standard-contractual-clauses-to-be-referred-to-cjeu.

[91] Safe Harbor Invalidation, Cooley LLP, https://www.cooley.com/news/insight/2015/2015-safe-harbor-invalidation (last visited on Apr. 2, 2018).

[92] The Swiss and U.S. also have a Privacy Shield Framework Agreement. Privacy Shield Overview, U.S. Dep't of Commerce, https://www.privacyshield.gov/Program-Overview (last visited Apr. 4, 2018).

[93] *Id.*

[94] *Id.*

[95] Cameron F. Kerry, *Trump Puts U.S.-EU Privacy Shield at Risk*, Brookings Tech Tank (June 14, 2017) https://www.brookings.edu/blog/techtank/2017/06/14/trump-puts-u-s-eu-privacy-shield-at-risk/ (Currently, the Privacy Shield is supported solely by an Obama executive order that extends privacy protections to foreign nationals. Repealing this executive order would result in a defunct version of Privacy Shield).

[96] *Id.*, (after providing an extension to the expiry period of FISA 2008 twice); Highlights of S. 139, as Amended The FISA Amendments Reauthorization Act of 2017 https://intelligence.house.gov/uploadedfiles/s_139_highlights_final.pdf [hereinafter Highlights of S. 139].

ing its content.[97] The amendments added a probable cause-based requirement to view data under Section 702 for FBI criminal investigations unrelated to national security and a new specific query procedure that builds on the foundation of the minimization principles.[98]

H.R. 4478 would widen the pool of individuals and organizations that could be searched by including those engaging in a vast range of cybercrimes, regardless of who actually accessed the computer.[99] While some feared H.R. 4478 would reauthorize the collection of "about target" data, the bill requires a mandatory and temporary cessation of "about target" collections for the foreseeable future.[100] The amendment leaves the door open and allows the Attorney General and the Director of National Intelligence to declare their intent to resume "about search" collections to congressional committees.[101] A 30-day period of congressional review would determine whether such searches should resume.[102] However, the ACLU fears that political gridlock will stop Congress from acting in time during such a period, resulting the codification of such searches.[103]

Efforts were made to include unmasking rules, a polarizing issue involving House Intelligence Chairman Devin Nunes claiming to have information relating to the Obama administration 'unmasking' names of the Trump's transition team within reports for political gain.[104] Under the minimization requirements of FISA, domestic citizens are not to be included except when the information is already public available, the intelligence information would not make sense without the U.S. citizen's identity, and/or when the U.S. citizen might be working with a foreign nation.[105] This leads to the potential abuse of revealing the identity of U.S. citizens who are unrelated to the search, violating their rights. Despite being exclude from H.R. 4478, the Director of National Intelligence issued new procedures detailing the approval process with a standard of "fact-based justification" and the need for a concurrence from the intelligence community general

---

97 Neema Singh Guliani, *NSA Surveillance Bill Would Dramatically Expand NSA Powers*, Am. Civ. Liberties Union (Nov. 30, 2017), https://www.aclu.org/blog/national-security/privacy-and-surveillance/new-surveillance-bill-would-dramatically-expand-nsa (those falling under the national security exception would greatly increase as 'malicious cybercrimes' are broadly defined and likely could include anything from smaller acts of piracy to terrorist communications and recruiting, regardless of whether the computer owner had committed the crime).

98 Highlights of S. 139, *supra* note 96; Karoun Demirjian, *House Intelligence Committee Passes spy-bill Renewal, But on Party Lines*, The Wash. Post (Dec. 1, 2017), https://www.washingtonpost.com/powerpost/house-intelligence-committee-passes-spy-bill-renewal-but-on-party-lines/2017/12/01/8aa2367e-d686-11e7-95bf-df7c19270879_story.html?utm_term=.4b86f9fd5bf3.

99 Guliani, *supra* note 97.

100 Highlights of S. 139, *supra* note 96; Daniel Wilson, *House Panel Approves Surveillance Renewal Bill* Law360, https://www.law360.com/articles/989972/house-panel-approves-surveillance-renewal-bill/; Guliani, *supra* note 97 (about data targets information specifically about a person, without looking into an individual's own communications or data).

101 Highlights of S. 139, *supra* note 96.

102 Amendment in the Nature of A Substitute to S. 139, 1, 23 (Jan. 19, 2018) https://intelligence.house.gov/uploadedfiles/s_139_text_as_amended.pdf.

103 Highlights of S. 139, *supra* note 96; Guliani, *supra* note 97.

104 Highlights of S. 139, *supra* note 96.

105 *Id.*

counsel to allow the unmasking of presidential transition team members in the days prior to H.R. 4478's renewal.[106]

IV. Analysis: A Breakdown in Herd Immunity: The GDPR Effects on Business and the Security's Field

Herd immunity is most effective when that critical number of the group is immunized.[107] In cyber security, the concept is illustrated well when analyzing the period of the DPD. EU member states that had weaker and inconsistent laws for protecting data were more exposed and allowed for major exploitation.[108] Without the consistent immunities throughout a majority of the member states, this patchwork of data protection laws were largely ineffective for the EU.[109] In creating the GDPR, the EU's goal to harmonize data laws, curb the effects of data breaches, and provide citizens with some control over their data is now being offered to the international community as vaccination in order to reach a new critical mass.[110]

To acquire the critical mass quickly, GDPR mandatory compliance begins on May 25, 2018 and there will be no trial period to test what methods are most effective.[111] American businesses and international data controllers that process EU data will bound to comply and held liable for breaches and potentially subject to the astronomically high fines.[112] The expectation by European lawmakers is that all businesses were aware of the compliance requirements and would have already mapped out their current data processing and data handling methods.[113] Such mapping may include isolation and identification of what information should be processed pursuant to the GDPR, which third party members are receiving information, allocating a budget in case of breaches and noncompliance with the new regulation, and implementing mechanisms that support data rights, such as Google Spain creating erasure request forms for their site.[114] These new procedures are expensive and require a massive number of employees to estab-

---

106 Press Release, DIRECTOR OF NATIONAL INTELLIGENCE, *DNI Coats Establishes New Intelligence Community Policy on Request for Identities of U.S. Persons in Disseminated Intelligence Reports*, (Jan. 11, 2018); Rebecca Shabad, *Director of National Intelligence Issues New Guidelines for Intel Report Unmasking*, (Jan. 11, 2018) https://www.cbsnews.com/news/director-of-national-intelligence-issues-new-guidelines-for-intel-report-unmasking/.

107 Willingham & Helft, *supra* note 1.

108 Scott J. Shackleford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Study*, 67 S.C. L. REV. 609 (Spring 2016).

109 Gilbert, *supra* note 17, at 819.

110 Caroline Krass, Jason N. Kleinwaks & Ahmed Baladi, *A GDPR Primer for US-Based Cos. Handling EU Data: Part 1* Law360, http://www.gibsondunn.com/publications/Documents/Krass-Kleinwaks-Baladi-Bartoli-A-GDPR-Primer-For-US-Based-Cos-Handling-EU-Data-Part-1-Law360-12-12-2017.pdf [hereinafter *GDPR Primer*] (through mandatory compliance).

111 GDPR Primer, *supra* note 96.

112 *Id.*

113 *Countdown to GDPR Compliance*, *supra* note 19, at 3-4.

114 *Id.*

lish and maintain a data processing system that complies with the GDPR.[115] For some Fortune companies, the technology alone will cost $1,000,000.[116] Companies are expected to maintain close watches over third parties and any information set to a third country must meet the adequacy test.[117]

The GDPR 'vaccine' will likely provide some benefits for international citizens. For example, data breaches that affect EU data will likely also affect all data process within a specific company, regardless of the separate systems for processing. With those breaches reported to the EU within 72 hours under the new requirements, the citizens and the governments will be more aware of the potential that data was stolen and can better monitor and respond to other potential threats.[118] Watchful eyes on third parties may alert companies to potential misuse of a user's data but 22% of U.S. companies reported that there was no budget established to support third party legal consequences.[119]

However, with the American data still under a separate system and with the questions about the enforceability of the fines, corners will likely be cut.[120] Any EU data processing automatically requires a company comply with the GDPR, meaning companies that rarely come into contact with data from the EU may be unaware of the potential fines and could be underprepared to protect information.[121]

While it might behoove some companies economically to create a single-tier system based on the GDPR, it is incredibly unlikely that U.S. businesses will adopt these standards for the American data. Currently, data, metadata, and information are huge commodities for both national security protections and for businesses.[122] Data demand is high and the analytics of that data reveals habits, needs, and opportunities to make money.[123] The data protections of the GDPR would limit the forms of data that could be transferred and would have to explain why that data was being transferred to the consumer, a process that would di-

---

[115] Tobias Bräugtigam, *How to Budget for a GDPR Project: A Primer*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Nov. 29, 2016) https://iapp.org/news/a/how-to-budget-for-a-gdpr-project-a-primer/; Tara Seals, *GDPR: True Cost of Compliance Far Less Than Non-Compliance*, INFO SECURITY GROUP https://www.infosecurity-magazine.com/news/gdpr-true-cost-of-compliance/; Ray Schultz, *The Price of Compliance: Study Uncovers GDPR Costs*, MEDIAPOST, https://www.mediapost.com/publications/article/309342/the-price-of-compliance-study-uncovers-gdpr-costs.html.

[116] *Fortune and FTSE Firms to Spend Millions Gearing up for GDPR Compliance, New Survey Show*, PAUL HASTINGS (Oct. 25, 2017)https://www.paulhastings.com/news/details/?id=1c74ed69-2334-6428-811c-ff00004cbded, [hereinafter *Fortune and FTSE Compliance*].

[117] *Id.*

[118] *The Equifax Hack*, *supra* note 51, (companies like Uber and Equifax would no longer be able to hide the hacks).

[119] *Countdown to GDPR Compliance*, *supra* note 19, at 3-4; *Fortune and FTSE Compliance*, *supra* note 108.

[120] Dellinger, *supra* note 40 (at this moment, there are questions as to whether the fines will even be enforceable on U.S. based companies).

[121] GDPR Primer, *supra* note 96.

[122] Vasuda Thirani & Arvind Gupta, The Value of Data WORLD ECONOMIC FORUM (Sept. 22, 2017) https://www.weforum.org/agenda/2017/09/the-value-of-data/.

[123] Alan Lewis & Dan McKone, *To Get More Value from Your Data, Sell it*, HARVARD BUSINESS REVIEW (Oct. 21, 2016).

rectly affect the profitability of the information that is being sold. If the data were to be stripped down and limited by what a company is absolutely allowed to have, the commodity price and its potential effectiveness are also diminished. Additionally, implementing the two-tiered system is economically advantageous because if consumers were informed each time their data was transferred and why, the economic viability of the data exchange would be reduced.[124] While the lowered value could revolutionize data protection, a two-tiered system subject to extensive fines for failures to comply leaves companies with less to invest in defenses.[125] With such unprotected security gaps, the herd of data processors is ultimately left exposed.

These same businesses would have to comport each of their multi-level, data security frameworks to a new set of regulations for data requests and still try to honor the data rights of its EU citizens.[126] The succinct collection of data under the right to data portability would benefit national security surveillance. When requested, businesses will simply hand over data and metadata crafted for the portability, including any additional inferences from the algorithms that would not have been included for the data subject. While placing the limits on the amount of time that a data controller may hold information decreases the chances of either the government requesting it or the information being robbed due to a hack, most information is never permanently deleted.[127] If "about target" collections were to allowed to resume, the collection of multiple data points from different data collectors could be synthesized and used to illustrate data as if it had been collected under the PRISM project, diluting the privacy protections of EU citizens under the GDPR.[128]

V. Proposal: Vaccination

As long as there is a disparity in the level of security used to protect European data from all other data, there will be strain on the resources that are utilized to protect such data. To alleviate the strain of the two-tiered system on the data protection, Congress needs to pass a permanent ban on "about target searches". International governments should involve their own citizens by implementing Fair Processing Requirements and the Right to be Informed from the GDPR.

By eliminating the "about target" searches, Congress would prevent the Executive branch from overstepping by collection information of foreign and domes-

---

[124] Joseph W. Jerome, Buying and Selling Privacy: Big Data's Different Burdens and Benefits STAN. L. REV. (Sept. 2013)("[A]ny given individual's data only becomes useful when it is aggregated together to be exploited for good or ill") https://www.stanfordlawreview.org/online/privacy-and-big-data-buying-and-selling-privacy/.

[125] Dellinger, *supra* note 40.

[126] *Countdown to GDPR Compliance*, *supra* 19, at 3-4.

[127] Kim Komando, *How to Delete Yourself From the Internet*, USA TODAY (June 23, 2017) https://www.usatoday.com/story/tech/columnist/komando/2017/06/23/how-to-delete-yourself-from-the-internet/102890400/.

[128] Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (Apr. 28, 2017) (the "about target" search has been referred to as a "backdoor search loophole").

tic individuals who are not the targets of the investigation themselves.[129] While other forms of data collection will still occur, by eliminating this egregious form, the data collected will more squarely fall in line with the GDPR's exception for national defense under Article 23, as at least one individual in the communication will be the suspected and targeted individual.[130]

Furthermore, by providing citizens with more consumer notifications on their data, the accountability would extend beyond the companies. When properly informed of the locale of the data and the intended recipients, citizens can provide a new level of inoculation to the protection scheme. By expanding Articles 13-15 of the GDPR to American data, consumers could take an active role in monitoring the intended data recipients and the protective measures during the data utilization.[131] While U.S. privacy allows companies to compile data under the First Amendment, notification of data utilization and the intended data users acknowledges consumers' concerns.[132] This would force companies to be more transparent. Transparency translates to accountability. Companies would be held accountable should a data breach occur.[133]

By melding in some GDPR data rights and restricting the 'about target' searches, the burden on companies to maintain a two-tier system will reduce and allow for more resources to go towards cyber defense.

VI. Conclusion

Data protection rights are most effective when each party is involved with processing, collecting, and updating the information, while protecting themselves through similar means. The GDPR offers the international community the latest inoculation to protect citizens' data rights. However, so long as broad exceptions to these rights exist and countries, like the U.S., have different privacy standards and data collection methods, an inoculation will be ineffective for attaining a critical mass to protect the herd. Adopting even some of the data rights gradually would provide the U.S. with an additional fighting chance on the battlefield of cyber warfare.

---

[129] *Id.*

[130] Drury & Hayes, *supra* note 41, at 819.

[131] GDPR, *supra* note 16, at Articles 13-15.

[132] Deckelboim, *supra* note 62, at 272.

[133] Yavorsky, *supra* note 43 (such as implementing higher levels of encryptions or pseudonymization to hide a data users' attributable features from the data).