Northwestern Journal of Technology and Intellectual Property

Volume 17 | Issue 2 Article 3

3-2020

DATA SECURITY IN A GLOBAL ECONOMY

John Butz
Northwestern University Pritzker School of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

DATA SECURITY IN A GLOBAL ECONOMY

John Butz

March 2020 VOL. 17, NO. 2

Volume 17, Number 2 (2020)
Northwestern Journal of Technology and Intellectual Property

DATA SECURITY IN A GLOBAL ECONOMY

John Butz[*]

ABSTRACT—This note examines the privacy and data security regimes in three distinct systems: that of the United States, the European Union and in India. The strengths and deficiencies of these three systems are analyzed and used as a foundation for imagining and articulating the importance of a global data privacy regime. The note argues that the nature of data protection requires a global system that balances the values of these three different systems. Despite the challenges of international cooperation and the different priorities that each of these areas has regarding data security, an international system would be beneficial compared to the current differing systems.

INTRODUCTION 261
PART I: THE UNITED STATES.....263
PART II: EU/GDPR 266
PART III: INDIA/AADHAAR.....271
PART IV: A GLOBAL FRAMEWORK.....274
CONCLUSION 278

INTRODUCTION

Social media corporations make up some of the largest companies in the world, and they work on a global scale. Data ownership and utilization make up a large portion of their revenues, yet the true value in this information can only be fully monetized when the identity of the user and the data that they provide and create can be matched.[1] The control that private companies have over data varies widely among different countries and regions. In the United States, privacy regulations are determined by different sectors of society and the regulations for the control of that information depends on the field to which it applies.[2] Unlike in the United States, where data ownership is largely controlled by user agreements, the European Union

[*] Northwestern University Pritzker School of Law, J.D., 2020.

[1] Nandan Nilekani, *Data to the People: India's Inclusive Internet*, FOREIGN AFF., Sept.—Oct. 2018, at 19, 24.

[2] Pam Dixon, *A Failure to "Do No Harm"—India's Aadhaar Biometric ID Program and its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.,* 7 HEALTH & TECH. 539, 551 (2017).

has recently enacted the General Data Protection Regulation (GDPR), which imposes much more stringent requirements on these companies.[3]

Backlash over recent scandals has caused Facebook to actively reconsider the way that it manages and shares the data of its users. As recently as March 6, 2019, Facebook CEO Mark Zuckerberg shared plans to add encryption elements to the posts, messages, and transactions that take place on Facebook and to automatically delete content posted on the site after a certain time period.[4] While some of these changes will protect Facebook from the legal, financial, and reputational harms that it has suffered recently, the legal landscape for Facebook and other global data companies is not settled and likely will not be established in the immediate future, as evidenced by the recent call to break up the big tech companies by Democratic presidential candidate Elizabeth Warren.[5]

The handling of these scandals and changes will require legal expertise that extends to the global scale on which these companies operate. Legal professionals who seek the lucrative business of working with some of the world's largest companies will need familiarity with, and footing in, regions with vastly different requirements regarding the data that makes these companies so valuable.

A third alternative system is being developed in India. While two private companies in the United States, Google and Facebook, have almost complete control over the ability to link user data to user identity, in India the government that is creating the system that will link its citizens to data created by technological advances.[6] In an attempt to modernize out-of-date and insufficient personal identification systems, the Indian government, in 2009, created the Aadhaar system.[7] The Aadhaar system assigns each Indian citizen who registered for the program a twelve-digit unique identification number and uses biometric verification, such as iris scans and fingerprints to confirm the identity of each user.[8] The program has grown rapidly since its creation, with over 1.21 billion unique identities now enrolled and ninety-seven percent of Indian citizens now possessing an Aadhaar number.[9]

---

[3] Nilekani, *supra* note 1, at 19.

[4] Joshua Rothman, *Mark Zuckerberg Announces Facebook's Pivot to Privacy*, THE NEW YORKER, https://www.newyorker.com/news/current/mark-zuckerberg-announces-facebooks-pivot-to-privacy [https://perma.cc/JC2G-WYJ8].

[5] Elizabeth Warren, *Here's How We Can Break Up Big Tech*, MEDIUM (Mar. 18, 2019), https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c [https://perma.cc/YL42-CZ8L].

[6] *See* Nilekani, *supra* note 1, at 24.

[7] *Id. at 21-22.*

[8] *Id. at 22.*

[9] *Id*.

Governmental implementation of this system has allowed it to be created as a public good, rather than as a method for generating revenue, which provides an incentive structure more aligned with public utility, but also raising privacy concerns.[10]

Part One of this paper will discuss the existing privacy controls in the United States, the ways that companies have failed to comply with even these relatively loose restrictions, and the role that lawyers and law firms have played in the fallout from these activities. Part Two will describe the effects and requirements of the GDPR and the way that law firms and lawyers have served to help businesses understand what will now be required of them under the new law. Part Three will describe the Indian Aadhaar system, in addition to some of the unforeseen legal consequences of its implementation. Part Four will examine the ways that the best parts of these three systems can be combined in the potential creation of a global data privacy framework. Part Five will conclude that the expansion of global data collection requires a global framework.

PART I: THE UNITED STATES

Some of the largest social media companies in the world, including Facebook, are based in the United States, where there is no federal data privacy regulation.[11] Individual states have their own data privacy statutes, and there are certain types of data for which the federal government does require protection (e.g., healthcare data, financial data, children's data, student data, and consumer information).[12] All of these regulations were created before significant personal use of the Internet, and therefore, are ill-equipped to fully protect these kinds of particularly sensitive information.[13]

Privacy regulation can vary state by state, which requires tech companies and other entities which control user data to conform to varying levels of protection depending on their location and the location of their users.[14] This can lead to companies either providing the highest level of security that is required in any state or different levels of security for different consumers based on what the law in that jurisdiction requires.

Both of these approaches lead to inefficiencies for the tech companies: first, because they are providing security beyond what is required in some areas, and, second, because they must use multiple systems and expend time

---

[10] *Id.* at 23-24.

[11] Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a new Paradigm in Data Privacy?*, 25 RICH. J. L. & TECH., no. 1, (2018), at 6.

[12] *Id.* at 17.

[13] *See id.* at 17-18.

[14] *See generally* Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 1963, 2013 (2018).

and resources maintaining multiple security platforms and working to determine when and where the right levels of security should be deployed. There are some areas where the laws in all fifty states overlap and create nationwide regulations without a federal privacy framework. The clearest example of this is in the area of Data Breach Notification, which requires companies in possession of user data to notify consumers when their personal information has been released.[15] The first instance of this type of regulation was a California law in 2003; the nationwide adaptation of this type of law took roughly seventeen years.[16] It should also be noted that even in this model case where Data Breach Notification has become the law throughout the United State, the definitions of personal information and the circumstances in which notification is required continue to vary state by state, leaving some of the same inefficiencies that exist in other areas of US data privacy law.[17]

The government agency that has played the largest role in regulating social media companies and the way that user data in the United States is used and shared has been the Federal Trade Commission (FTC), which is responsible for consumer protection.[18] The FTC successfully negotiated a settlement with Facebook, as recently as 2012, based on deceptive privacy settings and unauthorized sharing of user information and data.[19] A condition of this settlement is that "Facebook is barred from making misrepresentations about the privacy or security of consumers' personal information,"[20] however, this language has not kept Facebook from many further instances of reported misuse of consumer data.[21] The FTC does not have the authority to bring cases for violations of privacy: instead, they bring actions under consumer protection when corporations violate privacy or user agreements for deceptive trade practices.[22]

The most significant of these violations and resulting scandal in the United States is the Cambridge Analytica Scandal. During the 2016 Presidential Election, future president Donald Trump and his campaign hired

---

[15] *Id.* at 1963-64.

[16] *Id.*

[17] *Id.*

[18] G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 165 (2012).

[19] *FTC Approves Final Settlement with Facebook*, FEDERAL TRADE COMMISSION (Aug. 10, 2012), http://www.ftc.gov/opa/2012/08/facebook.shtm [https://perma.cc/CP6F-LKXU].

[20] *Facebook Settles FTC Charges*, FEDERAL TRADE COMMISSION (Nov. 29, 2011), http://www.ftc.gov/opa/2011/11/privacysettlement.shtm [https://perma.cc/T6PY-F5F9].

[21] Natasha Lomas, *Zuckerberg Refuses UK Parliament Summons over FB Data Misuse*, TECHCRUNCH (March 27, 2018), https://techcrunch.com/story/facebook-responds-to-data-misuse/ [https://perma.cc/65MK-EMJ3].

[22] Hans, *supra* note 18, at 164.

Cambridge Analytica, the political-data firm, which used Facebook data to predict voter behavior and suggest ways to use this information to influence them.[23] Facebook users consented to having information from their profiles shared with researchers for academic purposes when they agreed to a survey[24] (Facebook has discontinued this practice), but that data may not be sold or transferred to "any ad network, data broker or other advertising or monetization-related service."[25] An individual professor at Cambridge University sold the profile information intended for academic purposes, including location, of fifty million users to Cambridge Analytica.[26] Of those, only about 270,000 users are believed to have consented to the data transfer.[27] Congress has held hearings with Mark Zuckerberg as a result of this unauthorized sharing, and further reforms and adjustments are expected as Facebook continues to grapple with the damage to its brand and reputation from this scandal.[28]

During the fallout of the Cambridge Analytica scandal, Facebook faced numerous class action and privacy lawsuits. In response to these legal challenges, Facebook hired the law firm Gibson, Dunn & Crutcher LLP.[29] Gibson's privacy and cybersecurity practice was already considered one of the leaders in the field, having won favorable results for Yahoo!, and Uber, and also having a longstanding relationship with Facebook.[30] The notoriety and content of the Cambridge Analytica litigation was viewed by the practice group's leader Alexander Southwall as "particularly meaningful," and was described as involving the "most significant privacy legal issues of our day."[31] Facebook and Gibson Dunn are now in the process of fighting suits brought by shareholders alleging that the value of Facebook stock was negatively impacted by the scandal and class action lawsuits brought by

---

[23] Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, NY TIMES (MAR. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/6J2R-6LTJ].

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Lauren Feiner, *Mark Zuckerberg is Headed to Capitol Hill for the First Time Since Testifying About Cambridge Analytica*, CNBC (Sept. 18, 2019), https://www.cnbc.com/2019/09/18/facebook-ceo-mark-zuckerberg-visits-dc-to-discuss-tech-regulation.html [https://perma.cc/Q7SQ-23VP].

[29] Perry Cooper, *Facebook Taps Gibson Dunn to Handle Cambridge Analytica Fallout*, BIG LAW BUS. (Apr. 10, 2018), https://biglawbusiness.com/facebook-taps-gibson-dunn-to-handle-cambridge-analytica-fallout [https://perma.cc/W2CP-CBKK].

[30] Shayna Posses, *Cybersecurity & Privacy Group of the Year: Gibson Dunn*, LAW360 (Jan. 23, 2019), https://www.gibsondunn.com/wp-content/uploads/2019/01/GDC-PGOTY-Cybersecurity-Privacy-Group-Of-The-Year-Gibson-Dunn-Law360-01-23-2019.pdf [https://perma.cc/TDA6-8LM5].

[31] *Id.*

users.[32] Not surprisingly, Gibson Dunn is a global law firm with offices in ten different countries around the world.[33] This ability to function on a global scale is critical to their ability to meet the needs of a company with the global reach and ambitions that Facebook and other similar companies have.

PART II: EU/GDPR

In May, 2018 the European Union's General Data Protection Regulation officially took effect and changed the landscape of privacy and data regulation throughout the world.[34] The EU takes a fundamentally different approach to data privacy and ownership than the United States does; in fact, it considers the right to privacy an inalienable right.[35] The effects of the GDPR are not limited to the borders of the EU.[36] The rights of European citizens to control their personal data and the regulations that the GDPR creates apply to any corporation that controls the data belonging to citizens of the EU, regardless of whether those companies are based, or even have offices, in one of the EU member states.[37] This expansive reach means that the number of companies that fall within the reach of the GDPR goes far beyond the social media companies that are generally thought of as the main controllers of user data such as Facebook and Google, and includes any company that serves users in the EU and controls their personal data.[38]

The expansive reach of the GDPR across borders can be seen in the results of a PwC survey of American companies regarding their prioritization of compliance with the then upcoming regulation. The survey, published on January 23, 2017, showed that 92% of respondents considered GDPR compliance a top priority in their data-privacy and security agendas, and 38% of respondents stated that GDPR compliance was their single top priority in 2017.[39] The basis for this prioritization is likely influenced by the extensive penalties that a company could face for failure to comply with the privacy and consent requirements that it imposes. For "serious violations" the

---

[32] Amanda Bronstad, *Facebook Dubs Cambridge Analytica MDL 'Broadside' Against Business Model, Moves to Dismiss*, THE RECORDER (Dec. 6, 2018), https://www.law.com/therecorder/2018/12/06/facebook-dubs-cambridge-analytica-mdl-broadside-against-business-model-moves-to-dismiss/ [https://perma.cc/6G7N-TRWH].

[33] *See Offices*, GIBSON, DUNN & CRUTCHER LLP (2019), https://www.gibsondunn.com/offices/ [https://perma.cc/8LGL-WUR9].

[34] Houser & Voss, *supra* note 11, at 7-8.

[35] *Id.* at 11.

[36] *Id.* at 22.

[37] *Id.* at 64.

[38] *Id.* at 8-9.

[39] *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, PWC (Jan. 23, 2017), https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html [https://perma.cc/VP3K-NE6B].

European Data Protection Authorities can fine a company up to €20,000,000 or 4% of their global turnover, whichever is higher.[40] This level of financial liability puts any company that controls the data of citizens of the EU in danger, including the largest data owners who face liability in the billions of dollars.[41] These levels of fines necessitate that companies understand—and comply with—the requirements of the new regulation and that they are in compliance with it to avoid potentially ruinous fines.

Law firms have served as one of the bodies that help companies that control data of European citizens to understand the steps that they are required to take in order to protect themselves from this liability, both for their own clients and through public statements.[42] For example, in July 2016, DLA Piper released an article that served as a guideline to assist businesses in complying with the upcoming GDPR regulations.[43] The article emphasized who would be affected by the new regime: "[I]t will apply to US businesses that sell to, make services available to, or somehow target data subjects in the EU—even if those US businesses have no operations or affiliates in the EU,"[44] as well as specific steps that companies should follow in order to comply.[45] These steps include developing and maintaining a privacy policy that complies with the requirements of the new regulation, securing the data of EU users in a way that ensures the restriction of unauthorized secondary uses, and reviewing the existing data sharing agreements with third parties to make sure that they limit the use of data to specified purposes.[46]

Glory Francke of Davis Wright Tremaine LLP provided a similar open letter for businesses specifically regarding the requirements of companies' privacy statements in an article written for Law360.[47] She emphasizes that under the GDPR a company's privacy statement is a binding legal document, which, if violated by a corporation's practices, will create legal liability.[48] Companies' privacy statements should, as Francke puts it, "say what you do"

---

[40] Houser & Voss, *supra* note 11, at 8.

[41] *Id.*

[42] *See e.g.*, *Privacy Shield is Final: What it Means for Businesses*, DLA PIPER (July 21, 2016), https://www.dlapiper.com/en/us/insights/publications/2016/07/privacy-shield-is-final/ [https://perma.cc/7K6R-66Q9].

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] Glory Francke, *Time to Update Your Privacy Statement for the GDPR*, LAW360 (September 26, 2017), https://www.law360.com/articles/964037/time-to-update-your-privacy-statement-for-gdpr [https://perma.cc/K4V5-LCFA].

[48] *Id.*

and "do what you say," as is required by the new law.[49] Saying what you do means writing a privacy statement that informs users how their data will be used, and in particular disclosing with whom their personal data will be shared.[50] The transfer of data to a third party will not insulate a company from liability for improper uses. Data transferred to a third party must be done for a specific and allowed purpose, and must receive affirmative consent from the users whose data is being shared.[51] The privacy statement must explain the legal basis for the collection and sharing of data and it must do so in language that a reasonable person would be able to understand.[52] Unlike in the United States, a statement buried in an opt-in, click through user agreement written in indecipherable legalese will not suffice under the GDPR.[53]

Francke also recommends that companies show deference to user privacy in the privacy statement and in practice.[54] The specific suggestion that she makes in this regard is to use the phrase "personal data" rather than "personal identification information," given the broader statutory reach of "personal data."[55] Making an effort and using the correct phrasing will not insulate a corporation from litigation and fines under the GDPR, but it will help a corporation in the event that such litigation arises. Even in the new European system, corporations will be expected to police themselves to a certain extent, given the enormous amount of data that companies will continue to collect.[56]

This self-policing is included in the GDPR in the requirement for some corporations to appoint a specified data protection officer.[57] Article 37 of the GDPR requires companies to appoint a data protection officer under three different circumstances: 1) when the data processing is being done by a public authority other than a court; 2) when the core activities of an entity include processing operations that require regular and systematic monitoring of individuals on a large scale; and 3) when an entity's core activities consist of processing data on a large scale within special categories, or relating to criminal convictions.[58] This requirement will include the largest players in

[49] *Id.*

[50] *Id.*

[51] *See id. See also*, Ben Wolford, *What are the GDPR Consent Requirements?*, GDPR.EU https://gdpr.eu/gdpr-consent-requirements/ [https://perma.cc/HHS3-Q9UT].

[52] Francke*, supra* note 47.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *See id.*

[57] Houser & Voss, *supra* note 11, at 79.

[58] Commission Regulation 2016/679, 2016 O.J. (L119), art. 37 [hereinafter GDPR].

the tech industry who engage in systematic monitoring of individuals on a large scale. Facebook named Stephen Deadman as their Data Protection Officer on May 23, 2018.[59] Article 38 of the GDPR delegates the responsibility to the controller or processor to inform the data protection officer of issues related to the protection of personal data to support them in performing the tasks they are obligated to.[60] It states that data subjects may contact the data protection officer regarding all issues regarding their personal data.[61] Most importantly, it requires the independence and effectiveness of the data protection officer by requiring that the controller or processor does not give instructions to the data protection officer regarding their tasks and that they are not penalized by the controller or the processor for performing these tasks, and that they report directly to the highest management level of the controller or processor.[62] Further, Article 39 designates the responsibilities of a data protection officer and requires them to inform the controller or processor and the employees who carry out these functions about their obligations under the GDPR, to monitor compliance with it, to provide advice about the practices of the entity, to cooperate with the supervisory authority, and to act as the contact point for the supervisory authority.[63] Companies, especially those that control or process the data of European citizens, would be well-served to employ someone who meets the qualifications of a data protection officer, even if it is not clear that they fall under the requirements of the regulation. Given the expansiveness of the penalties that a corporation can face for noncompliance, this is a step worth the cost. The data protection officer is permitted to fulfil other tasks and duties, as long as they do not result in a conflict of interest—this will help smaller companies that may struggle to employ a data protection officer to comply with the GDPR.[64]

The most significant regulation introduced in the GDPR is the "right to be forgotten." This right allows private individuals the right to delete links to information about them, as well as permits deletion of their own postings online if they are able to prove that it serves no legitimate purpose.[65] This

[59] Caroline Spezieo, *Facebook Names Data Protection Officer as GDPR Deadline Nears*, LAW.COM (May 23, 2018), https://www.law.com/therecorder/2018/05/23/facebook-names-data-protection-officer-as-gdpr-deadline-nears/ [https://perma.cc/3K3E-7X2G].

[60] *See* GDPR, *supra* note 58, art. 38.

[61] *Id.*

[62] *Id.*

[63] GDPR, *supra* note 58, art. 39.

[64] *See* GDPR, *supra* note 58, art. 38.

[65] Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 354 (2015).

right also extends to public officials and figures.[66] The case that laid the framework for the "right to be forgotten" in the EU was *Google Spain v. AEPD*, in which a private individual sought to have Google remove links in a search of his name to an insolvency action from years before.[67] The court upheld his right to have this information removed, and in doing so, established the right of citizens of the EU to be "forgotten".[68] This did not mean, however, that the information that the citizen wished to be forgotten was erased or removed from the internet entirely.

First, there is the obvious irony of the fact that the information that the citizen wished to have removed from Google searches and "forgotten" is now attached to the most famous case relating to the GDPR, and thus, is a much larger part of the public consciousness than it ever would have been without this litigation. While future citizens who seek to have their information or data removed from the internet will not face the same level of recognition as the initial plaintiff, the law will be self-defeating if public record litigation is required to have information "forgotten." Second, this information was still stored in Google's files and remained accessible in searches from computers that did not have their domains in the EU.[69] The information was, therefore, not deleted or forgotten so much as made harder to find.[70]

The GDPR creates exceptions for when the right to be forgotten will be applied, thereby protecting some of the rights of expression and historical accuracy that run counter to a law requiring information to be hidden or removed from the internet. These exceptions are:

a) for exercising the right of freedom of expression in accordance with Article 80;

b) for reasons of public interest in the area of public health in accordance with Article 81;

c) for historical, statistical and scientific research purposes in accordance with Article 83;

d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence

[66] *Id.*
[67] *Id.* at 365.
[68] *Id.* at 364.
[69] *Id.*
[70] *Id.*

> of the right to the protection of personal data and be proportionate to the legitimate aim pursued.[71]

The GDPR does not provide information on when the right to free expression would overrule the right to be forgotten.[72] The meaning of these exceptions and when they apply will likely need to be sorted out through litigation. However, the right to be forgotten will naturally continue to run up against other rights of free expression and freedoms of the press.

Law firms will serve as points of contact for the companies they advise on how best to comply with these new and sometimes ambiguous regulations.[73] For smaller tech companies that are not able to afford the services of global law firms, this responsibility will likely shift to in-house counsel, who will rely on their individual expertise as well as the public materials that larger law firms have published. Also, global law firms themselves are subject to the regulations and controls of the GDPR, given that almost any law firm with EU-clients will have control over the personal data of their clients and opposing parties through discovery, due diligence, and normal business operations. This means that they will need to create policies for notification in the event of a data breach, have publicly stated privacy policies explaining the reasons for any data collection that they do, and disclose the sharing of personal data to any third parties and have compliant reasons for collecting such data.

PART III: INDIA/AADHAAR

The Aadhaar system was created in India as a method of identifying its citizens through biometric trackers, such as fingerprints and iris scans, that would theoretically prevent identity theft or misrepresentation.[74] The benefits to Indian citizens as a result of this program have been vast and significant, with Aadhaar identification being used to create millions of new bank accounts for residents who did not have the means to verify their identities before the system was created.[75] It has led to reduced corruption and fraud in government welfare and subsidy programs.[76] Many other benefits, such as linking healthcare data to individuals, are also now available.[77] The program

---

[71] *Id.* at 371.

[72] *Id.*

[73] Lisa V. Zivkovic, *The Alignment Between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject*, 28 TRANSNAT'L L. & CONTEMP. PROBS. 189, 206-07 (2018).

[74] *See* Nilekani, *supra* note 1 at 22.

[75] *Id.* at 22.

[76] *Id.*

[77] *Id.* at 26.

has also, however, created questions about the security of the information that is contained in the program and the ways that the government could use that data for improper uses, especially as the ubiquity and necessity of Aadhaar registration in India increases.

While at the time of its creation, the Aadhaar system was meant as a voluntary system that would be used for a limited set of governmental functions, it has quickly become a much wider functioning aspect of daily life in India.

> Initially the *Aadhaar* was only used for subsidies, now it is used for bank accounts, medical records, pension payments, and a seemingly ever-growing list of activities. While it was launched as *'voluntary,'* and for limited purposes, *Aadhaar* enrollment is now *'mandatory'* and must be present to receive many national government, and Indian State benefits and services. Additionally, *Aadhaar* enrollment has become both functionally and practically mandatory even beyond those levels.[78]

As the practical and legal ability of Indian citizens to opt out of the system shrinks, the controls and protections for users should grow with it. In the early stages of the program, however, this was hardly the case.

When the Aadhaar system was created and put into place, privacy was not established as a fundamental right of Indian citizens: "In the India example, there is simply no fundamental privacy redress for affected individuals."[79] Though some privacy protections did exist in the context of other technology legislation, these existing protections were not tailored to the enormity and significance of the Aadhaar program; "[a]lthough absent dedicated data protection legislation for the *Aadhaar* system, India has some existing privacy laws. These can be found in the Information Technology Act of 2000, which was amended in 2008."[80] These laws label certain kinds of information as "sensitive" and require user consent to share it.[81] Such sensitive categories include sexual identity, health records, passwords and, significantly, biometric information.[82] Even with these protections, however, the right of the government to share information internally and the ability of private corporations to access that information and use it to connect individual users to the data that those companies may have already collected, operated without a statutory framework for much of the early existence of the Aadhaar program.[83]

---

[78] *See* Dixon, *supra* note 2, at 542-43.

[79] *Id.* at 558.

[80] *Id.* at 547.

[81] *Id.*

[82] *Id.*

[83] *Id.*

Certain protections were built into the Aadhaar system that protected users from substantial breaches. The most significant of these is the fact that Aadhaar identification "is a 'dumb' ID, capturing less information about users rather than more. It knows only four data points about each holder: name, date of birth, address, and gender."[84] This is not the only way that the system was designed to protect some of the user's privacy: "Aadhaar incorporates privacy into its design in other ways, too. When a service provider sends an authentication request to Aadhaar, the purpose of the authentication is not revealed; all the government knows is when someone uses his Aadhaar number, not where or why."[85] These limitations concerning the government's ability to track the actual uses of Aadhaar identification and the limited amount of information that is actually contained within the database about a specific user provides some protections for users but is not a complete protection over governmental intrusions on individual privacy. By the very nature of the program, users are required to sacrifice any preexisting right to anonymity that may have existed. This is an especially high price to pay for people attempting to use government services in order to escape desperate situations, such as women attempting to use government resources to escape and rehabilitate from lives as prostitutes.[86]

These limited protections were the only avenues of protection for Aadhaar users until a landmark ruling in 2017 by the Supreme Court of India, which created a right to privacy for all Indian citizens.[87] This decision overturned two previous decisions holding that privacy is not a fundamental right of Indian citizens.[88] The holding also reinforced the idea that the program itself must remain voluntary.[89] However, as Aadhaar continues to expand its reach and functionality, this legal distinction will become increasingly obsolete.

Even with these existing and recently established protections, the true threat of the ways that the Aadhaar system could be used to threaten the privacy of Indian citizens is when an entity—either the government or a private organization—is able to combine the ability to identify individuals using their Aadhaar number with the functions for which that the number is being used.[90] In January 2018, a text program implemented by Facebook

---

[84] *See* Nilekani, *supra* note 1, at 24.

[85] *Id.*

[86] Dixon, *supra* note 2, at 557–58.

[87] *Indian Supreme Court in Landmark Ruling on Privacy*, BBC (Aug. 24, 2017), https://www.bbc.com/news/world-asia-india-41033954 [https://perma.cc/5247-UKMF].

[88] *Id.*

[89] *Id.*

[90] *See* Nilekani, *supra* note 1, at 23-24.

asked users to link their profiles with the name on their Aadhaar cards.[91] Similar requests have also been made by Amazon in order for users to track packages.[92]

India's decision to create the Aadhar system without installing adequate privacy protections is the greatest flaw in a program that has had generally positive results, creating opportunities and benefits for the overwhelming majority of its citizens, particularly, those who before its creation were left without ways to identify themselves to either the government or in their personal affairs.[93] In creating a system with such immense power over the everyday lives of citizens, restraint needed to be placed on the government's power before it was implemented: "More than any other factor, the underlying cause of India's current problems with *Aadhaar* are a result of the lack of appropriate regulation of the *Aadhaar* ID system before its widespread deployment into the Indian population. Legislating in reverse is extremely difficult."[94] The challenges that India will face as they work with an entrenched system will be much greater than if they had understood its ramifications, and protections had been in place that the system could have been created around. The fact that private companies are already taking steps to integrate the Aadhaar system into their products and platforms is the clearest indication of the dangers that could be created if these protections are ignored or not enforced. India will need to balance its interest in the functionality and ubiquity of the system against concerns about government overreach.

PART IV: A GLOBAL FRAMEWORK

Information spreads faster today than it ever has in human history. This trend is likely to continue as more devices collect data on their users, more systems are created for the harnessing and creation of this data, and the uses for this shared data become further refined and monetized. Data and information sharing is already taking place on a global scale. For regulation of the practices of technology companies and other data controllers to be as effective and as efficient as possible, the regulations—or at least a baseline of regulations—will need to be equally as global. However, global political realities will likely make this impossible. The United States, the world's

[91] *Facebook's Aadhaar Prompt was Meant to Check Fake Accounts, Not Collect User Data*, BUSINESS TODAY (Jan. 16, 2018), https://www.businesstoday.in/technology/news/aadhaar-prompt-facebook-connect-link-users-account-india/story/266891.html [https://perma.cc/N7PH-M8SJ].

[92] *Want to Open a Facebook Account? Keep Your Aadhaar Card by Your Side*, ECONOMIC TIMES (Dec. 27, 2017), https://economictimes.indiatimes.com/tech/internet/want-to-open-a-facebook-account-keep-your-aadhaar-card-by-your-side/articleshow/62267904.cms [https://perma.cc/55BD-ZYQQ].

[93] *See* Dixon, *supra* note 2, at 547.

[94] *Id.* at 562.

largest economy and the home of the vast majority of the largest technology and data firms, does not have an overarching federal data privacy regulation, much less the apparent will to commit to a binding global framework.[95] Despite the unlikelihood of its coming to fruition, this section will attempt to describe the way that a global data privacy law would function using the successful aspects and the failures of the three systems described in parts one through three of this paper.

In the United States, the FTC requires that when data controllers tell a customer that they are going to do or not do something with their data, they keep their promises and do not deceive users.[96] There are significant limitations on the effectiveness of these consent requirements under the U.S. system. The specifics as to what a user is consenting to can be buried within user agreements that people almost never read and can be written in a way most users will not understand, and if a company does not have a privacy policy, there are no limitations from the federal government on what they can and cannot do with the data that users give them.[97] Consumers do have the ability, however, to read the privacy statements that most data controllers do provide and decide for themselves if they want to consent to the terms that the company states, and to do so with confidence that once a company has committed to a policy, the FTC will require that they conform to it.

The most effective consent regulations among the three systems is that of the GDPR. The GDPR requires that consent to share data be affirmative.[98] It defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data."[99]

Importantly, the GDPR also requires that the privacy policy that companies provide be understandable to a reasonable person.[100] For consent to be meaningful, this is a necessary element. If users are not aware of, or cannot understand, that to which they are consenting, the functionality of this requirement is virtually useless. Should a global framework be established, it should adopt a similar requirement so that the consent requirement that exists across all three systems can effectively guarantee that people's data are not being shared or used in ways to which they are not aware that they have consented.

---

[95] *See* Rubinstein, *supra* note 14, at 1963.

[96] *See* Hans, *supra* note 18, at 169.

[97] *Id.* at 165.

[98] Houser & Voss, *supra* note 11, at 81.

[99] *Id.*

[100] Francke, *supra* note 47.

The requirement in the GDPR that data only be shared for specified purposes is far less likely to survive the scrutiny of any potential global regulation. The effectiveness of this requirement in the GDPR will play out in the years to come; however, even if it is successful, it is unlikely to become a requirement of a global privacy framework. The United States has fostered the rise of many enormous and successful technology and data-based companies and would likely want to give these companies more flexibility to distribute and utilize the data they collect than the GDPR currently allows for.

When governments themselves become players in the data sharing context, the need for regulation becomes even higher. India did not create significant restrictions to the way that they are able to use their identification system.[101] Thus, the result has been litigation and confusion about the requirements that the government face in their role as the entity with the strongest position to connect the individual citizens in their country with the data that they create.

The best example that can be seen from the three approaches discussed in this paper again comes from the GDPR. The GDPR places government entities that collect data, no matter their size or function, in the same category of requirements as it does the largest tech companies, as Article 37 of the GDPR requires that a data privacy officer be appointed to any public authority.[102] This shows that the EU is familiar with the ways that governments can and have used data on citizens for dangerous purposes. The data protection officers at these governmental positions have the same strict requirements that they do at corporations.[103] They are required to be independent of the organization, they must report to the highest level of decision makers there, they must serve as a contact point for the regulating authorities under the GDPR, and the organization must support them in efforts to conform with the requirements both in theory, as they create privacy statements, and policies, and in practice, as these statements and policies are enforced at the organization.[104] A worldwide data privacy framework should have at least these same conditions to restrict the power of governments over citizens' data.

One area of the GDPR that is unlikely to survive in a global framework is the right to be forgotten. Although the exceptions to when a person has the right to be forgotten pay homage to the right to free expression, it still remains unlikely that this right could functionally exist in the United States

[101] *See* Dixon, *supra* note 2, at 562.

[102] GDPR, *supra* note 58, art. 37(1)(a).

[103] *Id.*, art. 37 (3).

[104] *Id.*, art. 39.

under the First Amendment to the constitution. In *New York Times v. Sullivan* (1964), the Supreme Court of the United States upheld the right of the press to publish even false information about a public figure.[105] Ever since, the trends for freedom of expression, have only increased, and it is unlikely that a law allowing anyone, even a public figure, to have even untruthful information—much less truthful information—about themselves removed from a public source and pass constitutional muster. Given the economic size and the importance on the global stage of the United States, the government's unwillingness to create this right in the United States would likely keep this right from being part of a global data privacy framework. Even in a nonbinding capacity, the United States has shown reluctance to adopt a right to be forgotten or a similar regulation:

> Shortly after the European Commission released its proposal to the GDPR, the [Obama] White House released its own largely aspirational proposal, the Consumer Privacy Bill of Rights. Similar to the GDPR, it aims to strengthen privacy protection for online users to create trust in the online environment, which will stimulate economic growth and innovation. . . . However, President Obama's Consumer Privacy Bill of Rights does not contain an express or implied right to be forgotten.[106]

The inability to include a right to be forgotten is not likely to keep a global data privacy regulation from being effective. The right to be forgotten has many drawbacks and limitations that do not protect user data as much as they protect individual reputation. The inability to actually have a person or their actions be forgotten is an important reason why a global data regulation would not need to include this right. Even when the right to be forgotten is functioning in exactly the way that it is supposed to it is not a means to suppress a person's actions, statements, or online postings. There are many methods of keeping records of these things that do not require them to be searchable on Google or other similar online platforms. Offline electronic records, hard copy records, and human memory all serve to undercut the effectiveness of an attempt to allow a person to wipe the slate clean.

Given the three approaches to personal data protection that this paper has examined, the one that comes the closest to a potential global framework is the GDPR. Although it does not serve as a perfect model for what a global approach would look like, it provides the most comprehensive protections for users and is the most in line with the global values of consent for data usage and of restrictions on governmental control over user data. This regulation would face the immense challenges of needing to be rigid enough

[105] 376 U.S. 254, 286-88 (1964).

[106] Rustad & Kulevska, *supra* note 65, at 377-78 (footnotes omitted).

to protect the rights that people deem most important regarding data security, while being flexible enough to adapt to technologies that change and emerge at an exceedingly rapid pace. The challenge of creating such regulation and having it adopted by enough countries to make it effective will not be an easy one, however, as the impact of data control continues to enter the public consciousness the calls for such regulation will become stronger and stronger.

CONCLUSION

Given the speed of data transfers, the global reach of data access and the nature of information, global regulation would be the most effective means of protecting the interest of consumers who provide their information to data controllers. While the European Union regularly acts as a singular body, the fact that these countries have created uniform data regulations shows that there is some will to have overarching laws in this area. The need for controls is critically important when governments are a key player in the receiving of personal information or the identification of data users. The consent laws in the GDPR provide the most effective example of how a global regulation of data protection could function and serve the people whose data is being obtained.