The International Lawyer

Volume 52 | Number 3 Article 6

2019

C is for Cookie: Is the EU's New "Cookie Law" Good Enough to Protect My Data?

William A. Meyers

C is for Cookie: Is the EU's New "Cookie Law" Good Enough to Protect My Data?

WILLIAM A. MEYERS

I. Introduction

During the summer of 2017, Equifax, one of the three major credit reporting agencies in the United States suffered a data breach that exposed 143 million Americans to potential theft.[1] During the months of May through July, "sensitive personal information" including names, Social Security numbers, addresses, dates of birth, driver's license numbers, and credit card numbers were stolen by hackers with malicious intent.[2] In March of 2018, Reuters proposed that the cost of this breach could reach as high as 439 million dollars, making it the most expensive data breach in history.[3] Interestingly, that breach only affected 147 million consumers, but in 2018 it was topped by another devastating hack.[4] When Marriot asked its guests to check in, they would often require name, address, credit card information, and passport numbers.[5] In November of 2018, Marriot revealed that this personal information had been stolen in a data breach affecting up to 500 million guests.[6] This specific assault on personal data had been going on since 2014, and it galvanized lawmakers within the United States to publicly recommend data privacy laws that can discipline companies who fail in their cyber protection.[7] Senator Mark Warner, a Virginia Democrat, stated, "It is past time we enact data security laws that ensure companies account for security costs rather than making their consumers shoulder the burden and harms resulting from these lapses."[8] As devastating as these attacks were, neither of these data breaches were the largest in history. In 2013, Yahoo

1. Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMMISSION: CONSUMER INFO. (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

2. *Id.*

3. John McCrank & Jim Finkle, *Equifax Breach Could be Most Costly in Corporate History*, REUTERS (Mar. 2, 2018, 9:05 AM), https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257.

4. *Id.*

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

6. *Id.*

7. *Id.*

8. *Id.*

suffered a far more extensive data breach.[9] Yahoo initially believed this breach affected one billion users when it was discovered in 2016, but in 2017 they found the breach actually affected three billion users.[10] This is an astronomical number of individuals who were affected by a single data event. But as our world gets more dependent on technology and the Internet, and as long as companies make money collecting the data of users and monetizing it, this will become more frequent in the future. In fact, data breaches have consistently increased in recent years, with almost 1,300 breaches in 2017 and over 600 as of July 24, 2018.[11] This is obviously a problem that affects millions of people across the globe each year and is expected to continually increase as the global economy becomes ever more digital, forcing some to call for action.

While, according to Senator Warner, American citizens must shoulder the burden of these and the thousands of other data breaches that have occurred in the past few years, European citizens have a level of protection not enjoyed by those in the United States.[12] This is because of the General Data Protection Regulation ("GDPR"), also known as the "Cookie Law," which was passed in 2016 by the European Union ("EU") and effectuated May 25, 2018.[13] The GDPR is a sweeping regulatory reform regarding how organizations collect and store personal data and ushered in a new era of privacy protection in our online world.[14] On May 25, 2018—the day the GDPR was implemented—Facebook and Google were hit with an 8.8 billion dollar lawsuit, which just shows the seriousness of the GDPR.[15]

This comment will first dive into the history of data privacy in the European Union, as well as the history of the GDPR and its policies, ramifications, and effects on both the European marketplace and the global marketplace as a whole. Next, this comment will address if and how other nations will follow the European Union's lead when it comes to data protection and privacy or how their existing privacy laws compare with the GDPR. Lastly, the comment will speculate as to any potential legal developments as a result of the GDPR's implementation in the European Union and ways that it may evolve over time to affect not only the European Union but also other nations that do business in the European Union and

9. Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL STREET J. (Oct. 3, 2017, 9:23 PM), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804.

10. *Id.*

11. Axel, *Enough is Enough: 2018 Has Seen 600 Too Many Data Breaches*, MEDIUM (July 24, 2018), https://medium.com/@AxelUnlimited/enough-is-enough-2018-has-seen-600-too-many-data-breaches-9e3e5cd8ff78.

12. Nicole Perlroth et al., *supra* note 5.

13. Andrew Rossow, *The Birth of GDPR: What Is It And What You Need to Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#3c917d7855e5.

14. Rhiannon Williams, *Why 2018 Will be Remembered as a Turning Point for Tech*, INEWS (Jan. 1, 2019), https://inews.co.uk/news/technology/2018-turning-point-tech-facebook-google/.

15. Rossow, *supra* note 13.

those nations around the globe who have or are considering implementing data protection regulations similar to the GDPR, including the United States.

II. The GDPR

A. History of European Data Protection

The EU's data protection laws have for years been thought of as the gold standard when it comes to data protection.[16] According to Anu Bradford, professor of law and director of the European Legal Studies Center at Columbia Law School, the roots of data protection in Europe can be traced back to Nazi Germany in the 1930s and 1940s.[17] Bradford thinks a part of why Europeans are cautious about personal data is because the Nazis "systematically abused private data to identify Jews and minority groups."[18] After WWII, Germans in East Germany were still spied on by secret police who logged the personal information of citizens.[19] In response, the West Germany state of Hesse passed what is widely believed to be the first Data Protection Act in 1970, which was followed by a federal German Data Protection Act in 1977.[20] In 1983, in what became known as the *Census Decision*, the German High Court stated that the "personality right" includes "the authority of the individual to decide for himself, on the basis of the idea of self-determination, when and within what limits facts about his personal life shall be disclosed."[21] Part of the Federal Constitutional Court's reasoning is the fact that it is now easier than ever to acquire information and exert influence over another using that information and the psychological stresses that can accompany that kind of public awareness.[22] The court goes on to worry about a societal structure in which a citizen is unaware of who knows what about him/her, when they knew it, and why they knew it.[23] The court then states that "the individual must be protected from the unlimited collection, storage, use, and transmission of personal data as a condition for free personality development under modern

16. European Data Protection Supervisor, *The History of the General Data Protection Regulation*, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Aug. 16, 2019).

17. Olivia B. Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*, Time (May 24, 2018), http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/.

18. *Id.*

19. *Id.*

20. Edith Palmer, *Online Privacy Law: Germany*, L. Library Cong. (June 2012), https://www.loc.gov/law/help/online-privacy-law/2012/germany.php#_ftnref22.

21. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1. For a summary in English, see Donald P. Kommers, The Constitutional Jurisprudence of the Federal Republic of Germany 323 (1997).

22. *Id.*

23. *Id.*

conditions of data processing" and that the individual, not the state or some other power, has the right to determine if another party may use or divulge his personal data.[24] The Federal Constitutional Court does recognize there is a limit to this "informational self-determination," noting that the individual is a personality within a society and public interest may prevail over the rights of the individual in some cases (examples would be public safety or if an individual is missing).[25] According to Bradford, this case and the informational "self-determination" became the bedrock upon which the EU's views on privacy and data have been built.[26] These laws and this decision by the German Federal Constitutional Court set the stage for incredibly forward-thinking data privacy laws as the world becomes more and more digital.

In 1995, Germany's conservative approach to individual privacy permeated throughout Europe when the European Parliament enacted the Data Protection Directive.[27] The directive, which had baseline standards but not mandatory requirements for European nations (unlike regulations which are completely mandatory) and could be customized based on the needs of each individual nation, did not address digital storage, collection, or transfer policies.[28] Directives describe the minimum standards to which EU nations must comply, but each nation has the flexibility to implement it differently or adopt more strict standards.[29] As an example, Ireland had relatively weaker data protection laws and less government oversight than some other European nations under this directive.[30] The Data Protection Directive lacked the uniform policies and enforcement powers granted by the GDPR. The next development in European privacy law was before the GDPR in 2014 when Europe's top court, the Court of Justice of the European Union, affirmed the "right to be forgotten."[31] In this case, the court ruled that Google must abide by the wishes of users to take down or delete any data they had acquired that appeared to be irrelevant, inadequate, or no longer adequate to their business interests.[32] Since that decision, as of May 2018, Google has received more than 655,000 requests to remove roughly 2.5 million links, and they have complied with 43.3 percent of those requests.[33]

---

24. *Id.*

25. *Id.*

26. Waxman, *supra* note 17.

27. Rossow, *supra* note 13.

28. *Id.*

29. Alvar Freude & Trixy Freude, *Echoes of History: Understanding German Data Protection*, BERTELSMANN FOUND. (Oct. 1, 2016), https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/.

30. *Id.*

31. Waxman, *supra* note 17.

32. *Id.*

33. *Id.*

As technology has advanced, the need for a better regulatory framework became apparent to keep up with the innovations in technology.[34] A part of the solution for the EU was to pass the GDPR in 2016.[35] Many experts state that the GDPR is simply a modern upgrade to the Data Protection Directive based upon a better understanding of how data has been misused.[36] Additionally, unlike the Data Protection Directive, the GDPR is a regulation that is required to be enacted by all member nations in the EU.[37] To get a sense of the depth and specificity that the GDPR implements, the GDPR is composed of 173 recitals covering forty-five specific regulations on how companies should process data, forty-three conditions of applicability, thirty-five bureaucratic obligations for the EU member states, seventeen enumerated rights, eleven administrative clarifications, nine policy assertions, five enumerated penalties, and two technological allowances.[38] The goal of the GDPR is clear: data should serve mankind.[39] As the fourth recital of the GDPR states,

> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.[40]

B. The "Cookie Law" & Significant Reforms of the GDPR

The first recital of the GDPR states that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right."[41] According to the GDPR, "personal data" refers to "any information relating to an identified or an identifiable natural person ('data

34. *Id.*

35. *Id.*

36. Waxman, *supra* note 17.

37. Rossow, *supra* note 13.

38. Roslyn Layton & Julian Mclendon, *The GDPR: What it Really Does and How the U.S. Can Chart a Better Course*, 19 Federalist Soc'y Rev. 234, 234 (2018).

39. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2006 O.J. (L 119) 2.

40. *Id.*

41. *Id.* at 1.

subject')."[42] This idea of personal data protection as a fundamental right is influenced heavily by the Federal Constitutional Court's ruling in the *Census Decision*, and the GDPR also has two major protective rights influenced by historical European privacy principles.[43] First, the GDPR guarantees the right to erasure, or the right to be forgotten, which comes from the Court of Justice of the European Union's 2014 ruling.[44] Second, the GDPR guarantees the right of portability, allowing users to opt-in or opt-out of the data collection practices of businesses.[45] This gives individuals in the EU the ability to correct, access, and erase their data or move it to another service provider.[46] This is the reason for the "Cookie Law" moniker, as companies now request your consent before enabling web cookies, and they frequently do this by requesting your consent via pop-ups on their webpage once you visit the site.[47]

A cookie is a text file that gets downloaded to your computer whenever you visit a website that contains a site name and a unique user ID.[48] Once downloaded, the cookie allows websites to know that the user has been there before and can tailor the experience accordingly.[49] Cookies can be used for auto-filling forms, counting visitors, storing shopping basket items, personalizing content, targeting advertising, and recording user preferences, as well as for authentication and security.[50] The cookie aspect is a major change brought about by the GDPR, but there are several other aspects to the regulation that have significant effects on the cybersecurity of businesses who do business in the EU.

One way in which the GDPR has transformed cybersecurity is the punishments the regulation imposes on noncompliant businesses. The GDPR levies fines against businesses in two tiers: the first tier (which involves unfulfilled obligations by different parties responsible for data protection) will cost businesses the greater of 10,000,000 Euros or 2 percent of the previous fiscal year's global revenues.[51] The GDPR can also levy even higher fines against businesses for breaches of the basic principles of processing, the rights of the data subject, transfers, or non-compliance with a temporary order of the greater amount between 20,000,000 Euros or 4 percent of the previous fiscal year's global revenues.[52] This is in contrast, for example, to the United Kingdom's guidance under the Data Protection

42. *Id.*
43. Rossow, *supra* note 13.
44. *Id.*
45. *Id.*
46. Dan Frank et al., *Are You Ready for GDPR?*, WALL STREET J. (May 25. 2018, 12:01 AM), https://deloitte.wsj.com/cio/2018/05/25/6-ways-to-prepare-for-gdpr-2/.
47. Olivia Solon, *A Simple Guide to Cookies and How to Comply with EU Cookie Law*, WIRED (May 25, 2012), https://www.wired.co.uk/article/cookies-made-simple.
48. *Id.*
49. *Id.*
50. *Id.*
51. Regulation 2016/679, art. 83, 2006 O.J. (L 119) 82.
52. *Id.*

Directive where the U.K. had a max fine of 500,000 Pounds.[53] These fines could have devastating ramifications on a company that does not comply with the GDPR, but not every company is subject to it. To be subject to the GDPR, a company must fulfill four criteria: (1) an EU presence; (2) the company processes data of EU residents without a presence; (3) more than 250 employees; (4) and the data-processing impacts the rights and the freedoms of its data subjects even if there are fewer than 250 employees.[54] The GDPR defines data processing as

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[55]

Essentially, if a company does anything with your data in the EU or with the data of EU residents, they are subject to the limitations of the GDPR. This is a major overhaul that required significant time and cost by companies of all sizes in order to comply.

C. Cost to Implement the GDPR

The GDPR, designed to protect citizens' rights, "represents the most sweeping change to data legislation in decades."[56] Many think that it will become the new global standard for data privacy and security.[57] But reforms of this magnitude come at a significant cost. According to Ernst & Young, the world's 500 biggest corporations are on track (as of March 22, 2018) to spend a total of 7.8 billion dollars to comply with the GDPR.[58] Not only are companies working hard to ensure their software is compliant with the GDPR—like Microsoft, who has about 300 engineers working on its software to ensure it is compliant—there are other personnel decisions businesses must make to ensure they are complying with the GDPR.[59] For example, companies are required to appoint someone as the liaison to the

53. *GDPR Enforcement and Penalties*, IT Governance, https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (last visited Aug. 16, 2019).

54. Rossow, *supra* note 13.

55. Regulation 2016/679, art. 4(2), 2006 O.J. (L 119) 33.

56. Emily Busse, *Convergent Releases GDPR Capabilities for Ethics Cloud Platform*, Global Newswire (May 10, 2018, 9:00 AM), https://globenewswire.com/news-release/2018/05/10/1500368/0/en/Convercent-Releases-GDPR-Capabilities-for-Ethics-Cloud-Platform.html.

57. Expert Panel, Forbes Communications Council, *Adopting EU Data Protection Guidelines: Five Communications Experts Offer Ideas*, Forbes (Jan. 4, 2019, 7:30 AM) https://www.forbes.com/sites/forbescommunicationscouncil/2019/01/04/adopting-eu-data-protection-guidelines-five-communications-experts-offer-ideas/#4b0c12fc93b7.

58. Jeremy Kahn et al., *It'll Cost Billions for Companies to Comply with Europe's New Data Law*, Bloomberg Businessweek (May 22, 2018, 12:01 AM), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law.

59. *Id.*

EU's data protection regulators.[60] Additionally, many larger companies are required to appoint a "data protection officer" responsible for complying with the GDPR.[61] Another potential cost is monitoring. If data is lost or stolen for any reason, a business has only seventy-two hours to monitor the breach (no matter the reason), identify the cause, develop a report, and notify regulators.[62] These alone would be significant costs for companies, no matter the size, but they are not the only costs the GDPR requires for compliance.

Another hurdle that businesses will need to account for as they attempt to determine potential costs of complying with the GDPR is whether or not they are a controller or a processor.[63] According to the GDPR, a controller is "the natural or legal person . . . which, alone or jointly with others, determines the purposes and means of the processing of personal data."[64] According to Kyle Peterson, a simple definition of a controller is "a person who owns or functionally controls the personal data."[65] On the other hand, a processor is "a natural or legal person . . . which processes personal data on behalf of the controller."[66] Understanding the differences between a controller and a processor is important, because the answer defines what you are required to do under the GDPR, but in many cases a business can be both.[67] While their regulatory responsibilities differ, an important distinction is that processors take instruction or direction from controllers and do not have the right on their own to determine the purpose for which the personal data will be used.[68] Controllers are required to do several things under the GDPR. Controllers are required to give notice of a breach in data, follow specific contractual requirements when using a third-party processor, and design processes to protect privacy by default.[69] Processors have similar but slightly different responsibilities. Processors must notify the controllers of any breaches and must implement appropriate security measures to prevent any breaches.[70] Because many large companies can potentially be both controller and processor, this can be a very costly requirement to implement for the businesses and increases the cost of the GDPR.[71]

Not only will costs increase as companies reform their software, hire new people, and create individuals or groups to be in charge of the controller and

60. *Id.*
61. *Id.*
62. *Id.*
63. Kyle Petersen, *GDPR: What (And Why) You Need to Know About EU Data Protection Law*, 34 UTAH B.J., no. 4, Aug. 2008, at 12, 13.
64. Regulation 2016/679, art. 4(7), 2006 O.J. (L 119) 33.
65. Petersen, *supra* note 63.
66. Regulation 2016/679, art. 4(8), 2006 O.J. (L 119) 33.
67. Petersen, *supra* note 63.
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*

processor roles, but there are also a few other things these businesses must do to comply with GDPR.[72] First, companies must exercise increased record-keeping by identifying, inventorying, and maintaining records of all data on individuals based in the EU.[73] Additionally, companies are required to conduct "data protection impact assessments for any new processing or changes to processing demand to represent a high risk to the privacy and protection of EU resident personal data."[74] Companies also should evaluate their administrative, physical, and technical security capabilities and then improve their processes as necessary to accommodate any new risks that might have been discovered.[75] If the personal data of someone falls into the hands of a company's business partners, they could be liable for that as well.[76] But when the global cost of data breaches is estimated to be 2.1 trillion dollars by 2019, the GDPR would help mitigate much of these costs if it achieves one of its goals of preventing breaches.[77] Similarly, it is unlikely the cost of implementing the GDPR for a single company would outpace the fines that they could be subject to for noncompliance. So, it is likely in the best interest of at least major companies to ensure they are compliant with the GDPR due to the significance of the fines that could be levied against them.

D. Ramifications of GDPR Enactment

The GDPR has affected countless organizations in both the EU and abroad since its enactment earlier in 2018, and, in many cases, a strong understanding of the GDPR and what it requires does not exist.[78] Despite the somewhat limited understanding of the effects of the GDPR, several states in the United States—including California, Colorado, and others—have implemented laws giving individuals more power to demand that companies delete information that companies have stored regarding these individuals.[79] This move by states—and, possibly in the near future, other countries, including the United States—may have been premature, as there have been several unintended consequences of the GDPR since May of 2018.[80] Some think regional regulation of global technologies and

72. *Id.*

73. Frank et al., *supra* note 46.

74. *Id.*

75. *Id.*

76. *Id.*

77. Luke Irwin, *Global Cost of Data Breaches Will Rise to $2.1 Trillion by 2019*, IT Governance (August 30, 2017), https://www.itgovernanceusa.com/blog/global-cost-of-data-breaches-will-rise-to-2-1-trillion-by-2019.

78. Forbes Technology Council, *15 Unexpected Consequences of GDPR*, Forbes (Aug. 15, 2018, 9:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#422d938a94ad.

79. Kim S. Nash, *Good Privacy Requires Tech, Cultural Change*, Wall Street J.: CIO (Jan. 3. 2019, 10:50 AM), https://blogs.wsj.com/cio/2019/01/03/good-privacy-requires-tech-cultural-change/.

80. Forbes Technology Council, *supra* note 78.

companies will restrict privacy, freedom, and innovation, rather than enhance it, causing noncompliance and uncertainty.[81] For example, when the GDPR was implemented, it required users to explicitly opt in or out of allowing the company to use the data of the individual.[82] Facebook, which has built nearly its entire company on gathering data and selling it to advertising agencies or others, required a monthly fee to be paid if a user opted-out of allowing Facebook to use its data.[83] As a result, Facebook saw its user base decline, which could lead to a stagnation in innovation, as Facebook could earn less revenue from nations in the EU.[84] Others hypothesize that users will get tired of opting in on every website they visit so they will simply waive their rights without looking at the consents, which theoretically nullifies the need for some aspects of the GDPR if individuals do not know their rights and waive them anyway.[85] Some estimate that companies will spend 124 billion dollars in cybersecurity in 2019, which is a high cost if individuals are simply going to waive their privacy rights because they are tired of opting out.[86]

Another unintended consequence of the GDPR is the effect it has on small businesses.[87] Large companies, like Facebook, Google, Netflix, and others, have the requisite sophistication and cash to be able to accommodate nearly every regulation that is enacted.[88] However, this is not always the case with small, or even some medium sized companies, which subjects them to potential fines that could be crippling to their business.[89] And, according to Jason Straight, an attorney and chief privacy officer at United Lex, very few companies were ready for the GDPR on the enacting date.[90] Similarly, experts also expect that free services will go the way of the dinosaur.[91] For companies like Facebook, Google, and others, the data that they gather from their users is the product that they then monetize and sell.[92] If they can no longer collect or even monetize that data, they may require some payment for their services to offset that revenue.[93] In contrast, some hypothesize that this is only a good thing for Facebook and Google, as it is another barrier to entry because compliance with GDPR from the start will cost a lot of money, which some think will make Facebook and Google all the more

81. *Id.*

82. Bill George, *These Are the Challenges Tech Giants Will Face in 2019*, FORTUNE (Jan. 18, 2019), http://fortune.com/2019/01/18/big-tech-government-regulation-facebook/.

83. *Id.*

84. *Id.*

85. *See id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.*

90. Sarah Jeong, *No One's Ready for GDPR*, VERGE (May 22, 2018, 3:28 PM), https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu.

91. Forbes Technology Council, *supra* note 78.

92. *Id.*

93. *Id.*

valuable as they are able to dip into their nearly limitless resources to comply.[94] This means the big tech firms will just get bigger as startups and others may not attempt to enter the European market, because the cost of complying with the GDPR may simply be too high for a company to face in the early stages of their business.

Interestingly, pictures taken of individuals at work or at school are also included in the GDPR.[95] Even if schools or employees have permission to use those photos, every person in a photo has the ability to ask for the picture to be removed under the GDPR.[96] Additionally, data protection has now become an issue for even the most senior executives in the company, who are now responsible for the data processing of their companies, an area where few executives were well-versed before the implementation of the GDPR.[97] EU citizens will also suffer from reduced ability to access some technologies.[98] If a company is too small or not sophisticated enough to comply with the GDPR, they may simply refuse to offer their products to individuals in the EU or will simply deny access to EU citizens no matter where they are in the world.[99] Because individuals have the right to opt out of their data being used, another unintended (and perhaps dangerous) consequence of the GDPR is the inability to track cyber criminals.[100] These are significant ramifications, and, as GDPR enters its second year in effect in 2019, there are still other ramifications that have yet to be seen or considered. Regardless, as previously stated, there has been a push from other nations and states within the United States to implement something similar to a GDPR. But before this is done, some have presented ideas for improvements on the GDPR to improve economic efficiency and the interests of business in the global economy.

Some policymakers in the United States have deemed the GDPR not appropriate for the States for a few reasons.[101] The restrictions implemented by the GDPR are very demanding, and some argue this opens the door for selective enforcement.[102] The argument is that if the EU wanted to discipline companies like Facebook with the GDPR, but ignored punishing a huge percentage of organizations doing business in Europe who were not compliant with the new law, this may lead to selective enforcement of the restrictions of the GDPR. This selective enforcement would breed bias,

94. Jon Markman, *GDPR is Great News for Google and Facebook, Really*, FORBES (May 22, 2018, 11:57 PM), https://www.forbes.com/sites/jonmarkman/2018/05/22/gdpr-is-great-news-for-google-and-facebook-really/#5d57b24348f6.

95. Forbes Technology Council, *supra* note 78.

96. *Id.*

97. Adam Janofsky, *Under GDPR, Data Protection Officers May Help CEOs Stay Employed*, WALL STREET J. PRO CYBERSECURITY, https://cyber.pro.wsj.com/2017/08/18/under-gdpr-dpos-may-help-ceos-stay-employed/ (last visited Aug. 16, 2019).

98. Forbes Technology Council, *supra* note 78.

99. *Id.*

100. *Id.*

101. Layton & Mclendon, *supra* note 38.

102. *Id.*

corruption, or prejudice against larger companies while ignoring smaller ones.[103] These same doubters posit that strict enforcement of the GDPR could bring commerce in Europe to a halt as regulators may indiscriminately punish anyone who is not compliant with the GDPR; so, this necessarily selective enforcement may create that bias or strengthen companies like Facebook if Europe becomes desperate to ensure this giant company does business on the continent.[104] Perhaps it is in Europe's best interest to narrow the scope of the applicability of the GDPR to firms larger than it is currently; as of now many smaller business are still not GDPR compliant or have limited business in the EU as a result.[105] But this would be difficult, as theoretically the GDPR has nothing to do with the size of the company, but rather the sensitivity of the data. So, a small medical practice with 10 employees should be, by design, subject to all GDPR requirements due to the extreme sensitivity of the data that a medical practice would collect. Additionally, as stated previously, one of the unintended consequences of the GDPR is limited innovation which would be understandable in the country that developed Google, Facebook, Apple, Netflix, and many other tech giants.[106] But the state where many of these companies were developed (California) has already implemented its own state law that many have compared to the GDPR because of its "heavy-handed approach and potentially negative impact for enterprise."[107] Additionally, all of the states and territories within the United States have some sort of data protection law, be it simply a data breach reporting requirement or a comprehensive data protection framework like California.[108] It is clear that even if it is not the GDPR, data protection of some sort is important to state legislatures. It will be interesting to see if the federal government follows suit and implements its own data protection law and how extensive it may be. Will it be as extensive as the GDPR, California's law, or some other nation that has data protection laws less stringent than the GDPR?

III. Other Iterations of the GDPR Across the Globe

In June of 2018, California passed the California Consumer Privacy Act ("CCPA") which "gave consumers unprecedented protections for their data and imposed tough restrictions on the tech industry, potentially establishing

103. *Id.*

104. *Id.*

105. Kayla Matthews, *50 Percent of Firms Still Not GDPR Compliant: How About Your Data Center?*, DATA CTR. FRONTIER (June 22, 2019, 12:47 PM), https://datacenterfrontier.com/50-percent-of-firms-still-not-gdpr-compliant-how-about-your-data-center/.

106. Forbes Technology Council, *supra* note 78.

107. Layton & Mclendon, *supra* note 38.

108. Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT DATA PROTECTION REP. (June 22, 2019, 1:13 PM), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

a privacy template for the rest of the nation."[109] These regulations are the first of their kind in the United States; they will not go into effect until 2020 and can still be amended, but some legislators are hopeful that this will encourage other states or possibly the United States government to act and pass similar privacy regulations in their jurisdictions.[110] Even though the law only affects Californians, it is likely that tech companies will shift their policies to conform to the CCPA due to the difficulty of identifying and carving out conflicting standards between states or nations.[111] Despite the restrictions implemented by California, there are still significant differences between the CCPA and the GDPR.[112] The first major difference is the scope between the two agreements: the CCPA is mainly concerned with "effectuating data privacy rights by giving consumers knowledge concerning, and more control over, the collection and use of their personal information," while the GDPR's scope is much more expansive and includes personal data processing, the rights of data subjects beyond consumers, and accountability, just to name a few.[113] Other than scope, a few other significant differences are that the CCPA does not protect data that is publicly available and the CCPA applies to a narrower group of businesses—only those that are what the GDPR refers to as "controllers," do business in California, and exceed certain activity thresholds.[114] Perhaps most significantly, the CCPA presumes that data processing will happen and it is allowed; under the GDPR, data processing is unlawful.[115] The CCPA grants authority to the state attorney general to fine companies if they don't meet the standards.[116] The CCPA was not without its critics, however, who argue that it limits businesses' ability to use tools like customer loyalty programs because the law prohibits companies from treating individuals that opt out differently than those who do not opt out.[117] California is not the only state in the United States to enact data privacy laws, so while some consider this to be a template, it is possible that the United States, if it decides to implement a nationwide data protection law, may take some aspects from other state laws.

Japan's personal information protection legislation, which was passed at the beginning of 2016 and went into effect in 2017, had some significant

109. Marc Vartabedian, *California Passes Sweeping Data-Privacy Bill*, WALL STREET J. (June 28, 2018, 9:26 PM), https://www.wsj.com/articles/california-rushes-to-tighten-data-privacy-restrictions-1530190800.

110. *Id.*

111. *Id.*

112. JONES DAY, CALIFORNIA CONSUMER PRIVACY ACT GUIDE 18 (2018), https://www.jdsupra.com/legalnews/california-consumer-privacy-act-guide-13463/.

113. *Id.*

114. *Id.*

115. *Id.*

116. Vartabedian, *supra* note 109.

117. Marc Vartabedian et al., *Businesses Blast California's New Data-Privacy Law*, WALL STREET J. (July 1, 2018, 7:00 AM), https://www.wsj.com/articles/businesses-blast-californias-new-data-privacy-law-1530442800.

differences to the GDPR.[118] But after the GDPR was released, Japan and the EU agreed to recognize that each of their data protection regimes were adequate protections of personal data, creating what some described as the world's largest area of safe data flows.[119] In order for this to happen though, Japan had to be compliant with some of the articles of the GDPR, so Japan amended its privacy laws to ensure compliance.[120] The supplementary rules were announced in September of 2018 and included five substantive changes to the existing Japanese laws intended to tighten security of personal data and align Japan with the GDPR.[121] Some of the changes include the scope of personal information, the access right of consumers, succession of purpose of use, the retransfer of EU data after it has been in Japan, and anonymously processed information.[122] So while initially Japan's privacy laws were a bit different than those in the EU, they have been amended to ensure compliance and assist in data sharing between the two regions. Japan enacted a privacy law before the GDPR, but they were not the first nation in their part of the world to enact privacy legislation.

In September of 2011, South Korea enacted privacy legislation to protect its consumers, and it is considered by some to be one of the world's strictest privacy regimes.[123] Similar to the GDPR, it is a comprehensive protection of privacy rights for the data subject; it applies to most organizations, including governmental entities; and it includes penalties of criminal and regulatory fines with the possibility of imprisonment.[124] The purpose of this law is to "prescribe how personal data is processed in order to protect the rights and interests of all citizens and further realize the dignity and value of each individual."[125] The act aims to protect personal data from unnecessary collection, unauthorized use or disclosure, and abuse."[126] The law is similar to the GDPR in that it monitors any South Korean companies as well as companies that target South Korean consumers, but it does not distinguish between controllers and processors as both are considered personal information processors.[127] These processors include public institutions, organizations, individuals, etc. that either directly or indirectly process personal information to operate files of personal information for the official

118. Michiro Nishi, *Data Protection in Japan to Align with GDPR*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (June 23, 2019, 2:51 PM), https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr.

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. Alex Wall, *GDPR Matchup: South Korea's Personal Information Protection Act*, INT'L. ASS'N. OF PRIVACY PROFESSIONALS (June 23, 2019, 3:13 PM), https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/.

124. *Id.*

125. *Personal Data Protection Laws in Korea*, MINISTRY OF THE INTERIOR AND SAFETY, https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=1 (last visited Aug. 16, 2019).

126. *Id.*

127. Wall, *supra* note 123.

business of the company.[128] The South Korean law does not provide an exception for publicly available information, which is allowed in some cases under the GDPR, but does not actually define what a breach is and does not necessarily require notification of a breach, just that a company works to mitigate the breaches.[129] These significant laws in nations with developed economies have impacted businesses including imposing fines, regulation expenses, and legal fees to deal with as they need help to navigate these laws; and some companies have struggled in compliance with the GDPR specifically.

IV. Struggles with GDPR Compliance

The day that the GDPR was enacted, in May of 2018, four complaints were filed against Facebook and Google regarding their "take it or leave it" consent requirements.[130] The man who filed the complaints alleges these companies are using a strategy of "forced consent" to continue gathering personal data without giving users a choice of whether or not they want their data shared, which violates the GDPR's statutes.[131] Even more egregiously, Facebook has been accused of blocking the accounts of users who do not give their consent to collect their data.[132] Facebook released a statement following these complaints ensuring users that they will continue to improve their privacy policies and have implemented other changes to provide transparency with the data that they collect from their users.[133] Google, during the initial days of the GDPR, took a very conservative approach with user data, and as a result, was not able to sell personalized ads at each and every site that the user visits to prevent the hefty fines that can be levied under the GDPR.[134]

Despite this, less than a year into the GDPR, Google was fined nearly 57 million dollars because it failed to fully disclose what happens to users' personal information once it is collected.[135] The fine was handed down by France's data-privacy agency, CNIL, after a months-long investigation

128. *Id.*

129. *Id.*

130. Natasha Lomas, *Facebook, Google Face First GDPR Complaints Over 'Forced Consent'*, TECH CRUNCH (June 23, 2019, 4:21 PM), https://techcrunch.com/2018/05/25/facebook-google-face-first-gdpr-complaints-over-forced-consent/.

131. *Id.*

132. *Id.*

133. *Id.*

134. Nick Kostov & Sam Schechner, *Google Emerges as Early Winner From Europe's New Data Privacy Law*, WALL STREET J. (May 31, 2018, 5:30 AM) https://www.wsj.com/articles/eus-strict-new-privacy-law-is-sending-more-ad-money-to-google-1527759001?ns=prod/accounts-wsj.

135. Tony Romm, *France Fines Google Nearly $57 Million for First Major Violation of New European Privacy Regime*, WASH. POST (Jan. 21, 2019), https://beta.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.

beginning on May 25, 2018, which was the day the GDPR was enacted.[136] Google's platform—including Mail, Maps, Chrome, App Store, and YouTube—gives it a mountain of data that it could sort out, and even though Google gives the users the opportunity to change their privacy settings, the French did not think it was enough.[137] A data protection activist in France stated this is the first big signal about Europe's willingness to enforce the GDPR and it is a warning shot to all companies, significant not only for Google but for other companies as well.[138] This is the start of a new regulatory regime in Europe that effects many nations and companies around the world who do business there. There have been few fines enacted by the GDPR so far because the regulatory agencies are still investigating the complaints that have been levied against the companies.[139] In some ways, this is an example of the selective enforcement of the GDPR by regulators. When the GDPR was enacted, there was a very large number of companies that were not GDPR compliant and had not had any complaints or fines levied against them.[140] So, while Facebook and Google have received a lot of attention for their privacy policies (or lack thereof), other companies have been scrambling to correct their deficient privacy policies but have not had to deal with any repercussions for their failure to prepare, despite having well over a year to correct any deficient policies before the GDPR was enacted.[141] This is one of the "problems" that some lawmakers identified with the GDPR when it was first proposed and then enacted—inconsistent enforcement. But if the GDPR will simply target larger companies and forget about the small ones, will the GDPR be effective in the future, or will it just keep large companies from entering Europe? Will the EU consider rolling back the GDPR to have less of an impact on smaller companies in the future? It is probably too early to tell if the EU would even consider changing or amending its new law, but what about other nations? What is the future of international privacy law?

V. The Future of Privacy Law

The movement of the EU has, as previously stated, influenced the movement of other jurisdictions to enact or amend their existing privacy laws, including Japan, California, and several other states in the United States who have followed suit. The GDPR puts it this way:

---

136. *See id.*

137. *Id.*

138. *Id.*

139. David Meyer, *Here's Why the First GDPR Fines Could Still Be Months Away*, INT'L ASS'N OF PRIVACY PROF'LS (Aug. 28, 2018), https://iapp.org/news/a/heres-why-the-first-gdpr-fines-could-still-be-months-away/.

140. Sarah Jeong, *No One's Ready for GDPR*, VERGE (May 22, 2018), https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu.

141. *See id.*

> Rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data.[142]

These rapid technological changes, as well as the countless individuals whose data has been placed at the mercy of hackers, may put pressure on the U.S. federal government to enact their own privacy laws. Because the United States is one of the last major developed nations to not have a national data protection law, many are wondering if the United States will enact legislation and what form the law will take.[143] South Korea, Japan, and the EU already have them, so the United States is behind most of the developed world.[144] But if America decides to enact a privacy law, will it be as sweeping of a reform? Or will it be a less stringent and possibly a business-friendly approach? If the United States does enact a privacy law, there are a few key differences that it will likely have compared with the GDPR. It will likely be simpler, applicable to fewer companies (especially smaller ones), and will likely be a minimum standard that leaves significant flexibility for different states to enact more stringent requirements depending on the preferences of the states (similar to the initial directive implemented by the EU which served as the GDPR's predecessor).

A. Complexity of the GDPR

One of the largest complaints about the GDPR is its high standards which are difficult to police and hard for companies to comply with, because the requirements are seen by some as excessive.[145] As more nations attempt to enact privacy laws to safeguard the data of its users, many are wondering how they will be able to navigate the complexity of the law. The difficulty with the GDPR is weighing the benefits of protecting the data of all individuals while still ensuring the businesses that must comply still have the ability to invest in developing new technologies, jobs, and projects that will increase the quality of life for citizens, employees, and society as a whole.

---

142. Regulation 2016/679, 2006 O.J. (L 119) 2.

143. Tali Arbel, *Battle Lines Forming Ahead of Looming U.S. Privacy Law Fight*, Denver Post (Jan. 27, 2019, 1:00 PM), https://www.denverpost.com/2019/01/27/us-privacy-laws/.

144. Wall, *supra* note 123; Nishi, *supra* note 118.

145. *See, e.g.*, Layton & Mclendon, *supra* note 38.

One of the first problems with the GDPR is its complexity.[146] One company in London spent tens of thousands of dollars on consultants to ensure they were GDPR compliant only to be told they were already compliant and did not need to take further action because the data they collected was simple data.[147] The Chief Executive of this company complained about the complex nature of the law and lamented that even the consultants that he hired are still trying to figure the law out.[148] Some companies—like Tronc, Inc., a publishing company that owns the *Chicago Tribune*, *Los Angeles Times*, *Baltimore Sun*, and *New York Daily News*—have decided to simply block European users from accessing their websites at all.[149] One of the driving forces behind this decision was the level of complexity involved in attempting to interpret the GDPR and how some companies simply choose to avoid the GDPR altogether rather than attempt to interpret and spend the money to comply with the regulation.[150] In Tronc's case, Europeans do not have access to some news outlets in the United States, an important thing in our ever-growing and integrated economies. Some of the GDPR's provisions—like its insistence that data is collected and used for a specific purpose, and that the only data collected should be that which is necessary to fulfill that purpose—appear to be incredibly beneficial for individuals who use any website.[151]

But there are some obligations that are placed on businesses that are really difficult to implement and are also a burden on consumers who use several different services. For example, companies are required to ensure the personal data that they collect is kept up-to-date at all times; and while it is unclear exactly how this will actually be implemented or enforced, it is likely companies would need to regularly reach out to consumers to, at the very least, give individuals the opportunity to update their information.[152] Another difficulty is the idea that GDPR protections are supposed to follow the data if it is transferred to different nations.[153] In today's global economy, this is extremely difficult for an EU company to monitor, as it may have business partners in other nations that must now implement expensive

146. *See id.*

147. Sam Schnechner & Natalia Drozdiak, *From Restaurants to Insurers, the Race to Comply With New GDPR Privacy Rules*, WALL STREET J. (May 24, 2018), https://www.wsj.com/articles/gdpr-has-companies-big-and-small-racing-to-comply-1527154200.

148. *See id.*

149. Bethan Moorcraft, *LA Times and Chicago Tribune EU Exit Highlight Complexity of GDPR*, INS. BUS. AM. (July 10, 2018), https://www.insurancebusinessmag.com/us/news/cyber/la-times-and-chicago-tribune-eu-exit-highlights-complexity-of-gdpr-105578.aspx.

150. *See id.*

151. *What Data Can We Process and Under Which Conditions*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en (last visited Aug. 16, 2019).

152. *See id.*

153. *Id.*

GDPR compliance measures.[154] This is great if the ultimate goal of the European Union is data protection, but the stated goals of the EU are not necessarily data protection alone, but to uphold the interests of the EU as a whole.[155] This includes promoting peace, freedom, and prosperity.[156] The GDPR does promote the freedom of individuals to control their own data, but many will argue that it does not promote prosperity. While the GDPR is a step forward as it pertains to the protection of individual data throughout the EU, it hurts prosperity as companies are forced to spend billions of dollars on implementing the GDPR rather than doing things like creating jobs, growing their business, or improving returns for shareholders. It is likely that the companies that are affected most are those that do not even have shareholders, but rather small businesses who are now forced to spend much of their money on GDPR compliance — money that they may not have or would clearly be put to better use in growing their business or creating new jobs, so that the economy of Europe can grow as a whole.

B. Impact on Smaller Companies

Many opponents and proponents of the GDPR are interested to see the future of privacy laws and how they will differ from the GDPR. Many are especially interested in the future as it pertains to its treatment of small businesses and the harsh regulatory framework under which they are now forced to operate.[157] The GDPR imposes significant restrictions on small businesses, and some examples are particularly eye-opining as to the scope of the GDPR and how it impacts those businesses. One would think it is unlikely that a restaurant that has a single location in the United States would have to worry about GDPR compliance, but as EU residents make reservations when travelling to the United States and restaurants take down information to hold the reservation, they are now subject to the rules imposed by the GDPR.[158] Small businesses also are unsure how strictly the GDPR will be implemented and how much of an effort they need to put in to attempt to be compliant.[159] It may be in their best interests to simply risk non-compliance if the businesses think either the regulators will not enforce the GDPR against smaller businesses or simply accept fines, as they may cost less than actually hiring someone to ensure compliance with the GDPR.[160] It is likely that small businesses will simply follow the lead of big businesses and try, as best as possible, to implement a strategy that is similar to a big

154. *Id.*

155. *Overall Goals of the EU*, European Comm'n, https://ec.europa.eu/info/strategy/priorities-and-goals/overall-goals-eu_en (last visited Aug. 16, 2019).

156. *See* id.

157. Layton & Mclendon, *supra* note 38.

158. Schnechner & Drozdiak, *supra* note 147.

159. Pavol Magic, *How Small Businesses Can Survive in the Age of GDPR*, Entrepreneur (June 27, 2018), https://www.entrepreneur.com/article/315366.

160. *See id.*

business in their line of work so as to comply with the GDPR but cut costs while they do it by not hiring their own consultants.[161]

One of the differences in recent privacy data regulations (specifically California) is the requirement that if users do not want their data sold to third parties, they must opt-out.[162] The GDPR, on the other hand, encourages privacy by design or default.[163] Vermont requires companies that collect user data and sell it to third parties to register with the state and disclose if the user has the ability to opt out of the collection, retention, and sale of their data.[164] Each of these laws is more friendly to small businesses. If a restaurant in Vermont simply gathers information for its own use to enhance or streamline the reservation process, it would not need to register with the state and can simply gather that information to better serve its patrons. Similarly, the California law is a less drastic shift from typical business practices in the United States. Rather than forcing companies to completely shift their systems to privacy by design or by default, they can simply implement an option giving users the ability to opt-out.[165]

These are subtle changes in the framework of the law, but they drastically change the requirements for smaller companies. This enables them to make decisions that are beneficial for the consumers as it protects their data, but it also enables companies to make small, subtle changes to their practices while still retaining some flexibility to grow their business and better serve their customers. Even so, the increased cost of even a subtle change required to be compliant will be passed on to consumers, which might make the goods and services provided costlier to the customers.[166] These are particularly worrisome for small businesses who might not have the sales volume or margins of bigger businesses and may need to cut costs in other ways in order to retain their pricing strategies.

C. STATE FLEXIBILITY

If the United States enacts a data privacy law, which many legislators believe is necessary, it is possible it would serve a role that is more similar to the directive approach taken by the European Union before the GDPR. This would put a minimum requirement on the laws states would need to pass for data protection. States could go further, but, whatever states decide,

---

161. *Id.*

162. *What New U.S. Data Privacy Laws Mean for Business*, MARKETWATCH (Nov. 12, 2018), https://www.marketwatch.com/press-release/what-new-us-data-privacy-laws-mean-for-business-2018-11-12.

163. *What Does Data Protection 'By Design' and 'By Default' Mean?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (last visited Aug. 16, 2019).

164. *What New U.S. Data Privacy Laws Mean for Business*, *supra* note 162.

165. *See id.*

166. Niam Yaraghi, *A Case Against the General Data Protection Regulation*, BROOKINGS (June 11, 2018), https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/.

the legislators would need to ensure that the laws they develop meet a minimum standard. There is not yet a federal law on the books for data protection in the United States, but eleven states passed some sort of data protection laws in 2018, in addition to other states like California and Colorado which had already passed similar laws.[167] After these eleven states passed, updated, or continued to develop their data protection statutes, all fifty states in the United States, as well as D.C., Guam, Puerto Rico, and the U.S. Virgin Islands, have enacted breach notification laws that require businesses to let customers know if their personal data has leaked.[168] However, many of these states only have relatively simple breach notification laws on personal information and definitions of personal information.[169] Many states do not have the sophisticated data protection regime developed by California in 2018.

On January 15, 2019 the United States Government Accountability Office (GAO) recommended that the United States Congress consider developing comprehensive Internet privacy legislation to better protect U.S. consumers.[170] According to the report, the Federal Trade Commission (FTC) currently oversees Internet privacy, and currently the FTC directly enforces unfair or deceptive practices rather than promulgating and enforcing a regulation that has been enacted.[171] After the April 2018 Facebook data leak of 87 million users, the GAO was asked to review federal oversight of Internet policy (specifically the roles and responsibilities of the Federal Communications Commission (FCC) and FTC) and recommend a course of action.[172] After interviewing representatives from the industry, FTC and FCC staff, consumer advocacy groups, and officials from other federal oversight agencies, the GAO recommended developing "comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly changing Internet environment."[173] However, the GAO did not actually recommend what authority or agencies should oversee Internet policy, but it is likely that at the very least this will be explored by Congress in the near future.[174] This is a significant step in the United States developing a federal data protection law.

Legally, there are several spaces in the United States in which the federal government has deferred to states to regulate activities within their borders, several of which are in business. For example, the federal government allows

167. Serrato et al., *supra* note 108.

168. *Id.*

169. *Id.*

170. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 38 (2019).

171. *See id.*

172. *Id.*

173. *Id.*

174. *Id.*

states to regulate corporations, their own taxes, as well as allowing state banking charters.[175] Each of these has a significant effect on how businesses operate in their home states. A data privacy law is one that could be implemented and enforced similar to corporate law as it stands in the United States. For example, a company incorporated in Delaware is subject to Delaware requirements regarding corporate governance. Many companies incorporate in Delaware because of their corporate law, and it has become a competitive advantage for the state.[176] Could data privacy laws be implemented in a similar way? Could a business operate in the United States but be subject to a single state's data protection laws? This could become a competitive advantage for states as they attempt to draw businesses to their states. If a state has relaxed data protection laws that are cheaper to implement, businesses might move from their current state of incorporation and possibly reincorporate in a different state. However, based on the current regulatory environment, it is likely that instead the federal government may pass a sweeping regulation similar to the old EU directive: a minimum standard that must be met by all U.S. states, each of which can then add more stringent requirements on their own. For those states that lack a comprehensive data protection law, it is yet to be determined how complex these laws will be and what they will require of smaller businesses whose data protection is simple and used to only streamline certain processes. Regardless, it is clear that data protection is coming to many states, if not the federal government, in the United States.

VI. Is Data Protection Even Worth it?

Data breaches are becoming more frequent and more intense across the globe.[177] In the first half of 2018, data breaches increased by 133 percent from the year prior, which makes it understandable why some U.S. consumers and lawmakers are desperate to get some sort of privacy law passed in the United States, especially with some very early results from the GDPR.[178] The first fine under the GDPR was issued in Austria in October of 2018 for just under 5000 Euros.[179] Since then a German social media company was fined for not handling passwords correctly, and a Portuguese hospital was fined 400,000 Euros for allowing some of their non-medical

175. *A History of Central Banking in the United States*, FED. RESERVE BANK OF MINNEAPOLIS, https://www.minneapolisfed.org/about/more-about-the-fed/history-of-the-fed/history-of-central-banking (last visited Aug. 16, 2019).

176. *Why Businesses Choose Delaware*, DELAWARE.GOV, https://corplaw.delaware.gov/why-businesses-choose-delaware/ (last visited Aug. 16, 2019).

177. *What New U.S. Data Privacy Laws Mean for Business*, *supra* note 162.

178. Ed Targett, *6 Months, 945 Data Breaches, 4.5 Billion Records*, COMPUTER BUS. REV. (Oct. 9, 2018), https://www.cbronline.com/news/global-data-breaches-2018.

179. Mark Kiser, *Google v. GDPR: The Ripple Effect of the Biggest Data Protection Fine to Date*, TECHRADAR (Feb. 18, 2019), https://www.techradar.com/news/google-vs-gdpr-the-ripple-effect-of-the-biggest-data-protection-fine-to-date.

staff to access patient medical records.[180] These are the privacy violations or sloppy data protection practices that the GDPR was implemented to prevent, and as these fines begin to take effect and encourage companies to adopt or change business practices, the power of GDPR and data privacy regulation only continues to grow.[181] This was followed by the fine on Google in January 2019, indicating that, even though the penalty handed down to Google was not as severe as it could have been, these fines are only going to increase in frequency until companies appropriately adopt data protection policies that comply with the GDPR and that the GDPR, or privacy regulation generally, is here to stay.[182]

But do people really care that companies are collecting their data? In 2007, research was done that shows even though individuals complain about sharing their personal data, they freely provide it to companies to access the goods and services these companies offer.[183] Researchers explored this "privacy paradox," or the intentions of individuals to disclose personal information and their actual personal information disclosure behaviors.[184] Marketers seek to know their customers, leading to incredibly efficient communication with consumers targeting them for specific products and services based on their preferences.[185] The ability for companies to target consumers based on their preferences exposes them to products and services they would have otherwise not seen before, and consumers may decide to disclose more information so companies can cater their advertising to consumers more effectively. If this really is true—if individuals by and large do not care that companies are collecting their data—is the price paid to implement privacy laws truly worth it? People freely give their personal information and allow it to be collected by things like Facebook, Google Chrome, or Amazon's Alexa, and they do it to access the superior products or the benefits of these services at a lower price.[186] It could be argued that not one of these services is necessary to navigate life, and yet many people use them anyway. If individuals were truly wary of what companies did with their data, would they not try, as best as possible, to avoid these services or submitting their personal information to other, similar companies?

Even if the ultimate solution is as simple as disconnecting from these services, it is easier said than done. In today's connected world, where things like Internet browsers, email, and smart phones are essentially a requirement to be a good employee and to get business done, it is highly unlikely that an individual can disconnect from even most of these services where their data is being collected. These technologies do not even include so many of the

180. *See id.*

181. *Id.*

182. *Id.*

183. Patricia Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. OF CONSUMER AFFAIRS 100, 101 (2007).

184. *See id.* at 100.

185. *Id.* at 100 – 01.

186. Yaraghi, *supra* note 166.

things that are meant to make our lives easier like smart home speakers, wearable technology, 5G, and companies like Netflix looking at what individuals are watching. This is why these legislators have passed these laws. Companies today are doing everything they can to get you addicted to their products.[187] If the general public is essentially required to use this technology for business and are addicted to it in their personal use, then it could be argued that data protection is a requirement to protect consumers while their data is being collected from nearly every angle, packaged, and sold so that corporations can convince you to buy more of their products. New data protection laws also safeguard our data like never before; and in today's increasingly connected world, this is more of a requirement than ever.

The GDPR is the gold standard in data protection; it is likely to be a good thing for the citizens of the EU, and it is likely the rest of the world will follow suit. Whether or not the extensive requirements of the GDPR are a good thing for business is still to be determined, but it is clear that some sort of data protection regime is coming (or here) even if it does not go as far as the GDPR. As more nations either adopt GDPR like statutes, make their existing statutes compliant with the GDPR, or develop their own from scratch, it will be interesting to see how data protection laws effect businesses and how businesses continue to develop technologies that make our lives easier through innovation. While the GDPR is a new law with many of its repercussions or ramifications not yet understood or fully grasped, it is important, as data protection grows beyond the borders of the European Union, that businesses are still allowed to flourish and grow. Businesses encourage innovation and improve the prosperity of society, so balancing these seemingly competing interests will be increasingly important as data privacy regulation grows. Regardless, the GDPR is a step in the right direction in preventing data breaches and compromising situations for consumers.

187. Allen Kim, *How Tech Companies Are Addressing Screen Addiction*, CNN (Nov. 6, 2018), https://www.cnn.com/2018/10/10/tech/apple-google-facebook-tech-screen-addiction/index.html.