TRACKING FOOTPRINTS: THE NEED FOR STRONGER DATA PROTECTION LAWS IN THE DIGITAL AGE

*Abbigail Forrest**

INTRODUCTION 428

II. DATA PRIVACY IN THE DIGITAL AGE: A GROWING PROBLEM 430
- *A. The TikTok Problem: The World's Introduction to Data Privacy Concerns* 430
- *B. The Poor State of Data Protection in the United States* *431*
- *C. The Vast Impact of Data Privacy* 432
- *D. The Legal Landscape of Data Privacy in the EU and the US* 433
  - *1. The GDPR: The Future is Here, and it is Mostly an Improvement* 434
  - *2. The Spreading Legislative Impact of the GDPR on the United States* 437
  - *3. The Abysmal State of Data Privacy in the States: Over-Surveillance* 438

III. THE IMPACT OF THE EU'S DATA PRIVACY LEGISLATION, AND WHY THE WORLD MUST FOLLOW SUIT 439
- *A. The Benefits of More Extensive Data Privacy Laws* .. 439

* J.D., 2025, University of Houston Law Center; B.A., 2021, Texas A&M University. Houston Journal of International Law, Executive Editor, Board 48. Thank you to Board 49 for your time and efforts on this article. I would also like to thank my fellow editors on Board 48 for being a wonderful team to work with; and, finally, I wish to express my gratitude to my family and friends for their encouragement during this process and throughout my time at the Law Center.

1. Users in Control? Public Attitudes Towards Data Privacy 442
B. The GDPR and the US: its Impact, Implications, and Issues 443
1. What Has Made the GDPR So Effective? 445
2. The TADPF as a Measure of the GDPR's Impact in the United States 446
3. A Coming Storm for the TADPF? 449
C. An American GDPR: Federal Legislation, Speculation, and Existing State Laws as a Roadmap 450

IV. CONCLUSION 453

INTRODUCTION

As the Internet continues to permeate every aspect of modern life, new issues rise to the forefront of legal discussion: an important one concerns what can and should be done with the data that users put out into the digital sphere.[1] Legislation concerning digital data privacy and the widespread use of consumer data on the Internet is incredibly new, even though the first data protection laws came about more than fifty years ago.[2] This article will attempt to give an overview of some of the concerns with digital data privacy in the United States ("US") and the European Union ("EU"), as well as focus on the implications of new regulations. Most importantly, however, I will argue in favor of legislation and regulations that create higher standards for data privacy for both corporations and governments.

At first, it may seem like data privacy is not something that impacts the average person daily. But consider: when was the last time you received an email saying your phone number or email address was leaked in a data breach? How often have you been

1. The majority of data privacy and protection legal concerns began in the 1990s, and one of the earliest mentions of computers in the context of consumer data was in 1973. *See History of Privacy Timeline*, UNIV. OF MICH., https://safecomputing.umich.edu/privacy/history-of-privacy-timeline (last visited Oct. 25, 2023).

2. *See id.* (Establishing that laws directly addressing data privacy first started to spring up around fifty years ago).

browsing social media when an ad pop up for an item or service that you had *just* been talking to a friend about, but never searched for—or, on the other hand, have you looked up a specific product and continuously received ads for similar products for hours after? Data privacy is a relatively new concern, based almost entirely on the population's use of digital spaces, and because of that—at least in the US—there are very few restrictions on what can be done with user data. User data, in this case, not only includes what one puts about themselves online, but also includes the history of everything they have interacted with digitally, pages they have visited, and, most importantly, a portfolio of an individual's preferences created by a company interacting with this data.[3]

To start, I will address the topic of data privacy generally, as well as how it recently became a prominent issue in the US[4] and abroad due to the use of user data by social media applications. Following that, this article will provide an overview of the current state of data privacy laws in the US and the EU. Specifically, I will address the impact of the lack of federal data privacy laws in the US, the General Data Privacy Regulation ("GDPR") in the EU, and the emerging agreements between these two entities. To analyze data privacy, I will: discuss the impact of the GDPR, advocate for stronger data protection laws in the US and abroad by addressing the benefits of such laws, examine what changes the GDPR has sparked in the American system, and, finally, speculate on what a federal law akin to the GDPR could look like if implemented in the US. Through all this, I will argue that the US, as well as other countries, need to follow in the footsteps of the EU by enacting general data privacy legislation. As the digital sphere continues to grow, so does the need for protection of user rights and privacy. Data privacy laws are a necessary step for

3. *See* Chen, *infra* note 61; *see also* Mustri et al., *infra* note 62, at 2–3 (describing the method by which targeted ads are implemented, as well as what consumer data consists of).

4. Actions taken by the US federal government since the time this article was written (Spring 2024) are beyond the scope of this article and will not be addressed. *See generally* David Hamilton, *How TikTok Grew From a Fun App for Teens Into a Potential National Security Threat*, AP NEWS (Jan. 19, 2025), https://apnews.com/article/tiktok-timeline-ban-biden-india-d3219a32de913f8083612e71ecf1f428.

protecting citizens, businesses, and for securing the future of digital existence.

II. DATA PRIVACY IN THE DIGITAL AGE: A GROWING PROBLEM

A. *The TikTok Problem: The World's Introduction to Data Privacy Concerns*

Over the past couple of years, TikTok as a social media platform has been both a hot-button issue and an introduction to the topic of data privacy for many. Most of TikTok's controversy is centered around the access (or lack thereof) that the Chinese government has to the data of international users.[5] As a response, the United States has seen legal action taken to ban the platform in certain states, such as Texas.[6] While most have not fully banned TikTok (or are unable to), others have taken measures to prevent the platform from being downloaded on government-owned devices, including those used on some college campuses.[7] TikTok's CEO testified in front of Congress in early 2023 and offered a compromise: TikTok would build a facility in Texas to store American users' data and prevent the Chinese government from accessing it entirely, thereby "acting as a firewall."[8] However, this proposal did not do much to eliminate concerns from legislators, and ongoing challenges to the platform still primarily focus on what is done with the data it gathers from its users.[9] Furthermore, these concerns are not unique to TikTok

5. *See* Sapna Maheshwari & Amanda Holpuch, *Why Countries Are Trying to Ban TikTok*, N.Y. TIMES (Aug. 16, 2023), https://www.nytimes.com/article/tiktok-ban.html (describing the international state of TikTok bans, as well as delving into why countries may be deciding to enact such bans).

6. *See, e.g.*, David Shepardson, *US Judge Upholds Texas TikTok Ban on State-Owned Devices*, REUTERS (Dec. 12, 2023), https://www.reuters.com/legal/us-judge-upholds-texas-tiktok-ban-state-owned-devices-2023-12-11/.

7. Maheshwari & Holpuch, *supra* note 5; *see* Shepardson, *supra* note 6.

8. What, if anything, TikTok is doing or can do with the data it collects (beyond the scope of what is normal for a platform of its size) is unclear, and beyond the scope of this comment. *See* Dara Kerr, *Lawmakers Grilled TikTok CEO Chew for 5 Hours in a High-Stakes Hearing About the App*, NPR (Mar. 23, 2023), https://www.npr.org/2023/03/23/1165579717/tiktok-congress-hearing-shou-zi-chew-project-texas.

9. STEPHEN P. MULLIGAN, CONG. RSCH. SERV., LSB10940, RESTRICTING TIKTOK (PART I): LEGAL HISTORY AND BACKGROUND (2023) (establishing that the controversy surrounding TikTok is still an issue being debated in Congress).

as a platform, nor are they isolated to the United States.[10] Bans have been implemented internationally, sparking a new wave of questions pertaining to what companies do with the data they collect from international users.[11] TikTok's practices with user data are not unique either — Twitter, Facebook, and most (if not all) other platforms also gather the data of their users and use it to help improve their operations, or simply make a greater profit from ads.[12]

Many of the most inflammatory remarks made by policymakers are rooted in xenophobia and reactionary politics, which makes assessing the actual risk of the situation difficult.[13] Such rhetoric may also serve to deflect and distract from similar uses of user data by American corporations, as described above. Although complex, the situation with TikTok has brought the data privacy issue to the forefront of the discussion surrounding technology. While the rhetoric and reactions surrounding TikTok are not within the scope of this article to dissect, they are essential factors that may be influencing the ideas and opinions of the political leaders involved in the decision-making process.

B. The Poor State of Data Protection in the United States

Personal data can be used by government entities for a variety of reasons. For example, the US indicates that it uses consumer data as a form of surveillance in the name of national safety and counterterrorism, and much of its existing data privacy

10. Kerr, *supra* note 8.

11. Maheshwari & Holpuch, *supra* note 5.

12. One of the most common ways for a platform to make a profit from its users' data is to sell it to advertisers so that they, in turn, can create targeted ads to better sell products to users. Maheshwari & Holpuch, *supra* note 5; Aisling Redden, *Companies Are Collecting Your Personal Data. Here's What You Need to Know*, EURONEWS (Aug. 14, 2023), https://www.euronews.com/next/2023/08/14/companies-are-collecting-your-personal-data-heres-what-to-know.

13. Because TikTok's parent company, ByteDance, is still under the purview of China's broad surveillance laws, which could allow the country to access the data of users worldwide, many policymakers have heightened concerns. *See* Brian Fung, *Asian Americans Are Anxious About Hate Crimes. TikTok Ban Rhetoric Isn't Helping*, CNN BUS. (Mar. 27, 2023), https://www.cnn.com/2023/03/26/tech/asian-americans-tiktok/index.html (describing the situation regarding the possibilities of TikTok's use of user data as well as delving into the greater context of many proponents of bans of the platform).

legislation is made with these goals in mind.[14] Consumer data can also be used for other political means—for example, an election in Brazil was found to have been manipulated through the use of consumer data in deciding who to target with political ads on a common messaging app.[15] Overall, the current state of data privacy in the US is rather sparse. There is no general federal privacy law dictating what can and cannot be done with the data produced by the country's citizens, even though certain areas are more regulated than others.[16] In general, laws related to data privacy in the US tend to prioritize public safety, in contrast with those in the EU which focus more on the right to privacy of the individual.[17]

C. The Vast Impact of Data Privacy

Improved data privacy laws may not result in a dramatically different experience online for the ordinary user. The most visible results would likely be fewer personalized ads, the ability to see what is done with the data one provides through use of a specific platform, and fewer pop-ups asking for permission to use cookies.[18] The goal of efficient and well-written data privacy laws should be that the end-user's experience is as smooth as possible

---

14. Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022). One example of this is the Foreign Intelligence Surveillance Act ("FISA"), a controversial law allowing for extensive communications surveillance which will be discussed in detail in a later section. *See* Goitein, *infra* note 46; *see also* LINEBAUGH & LIU, *infra* note 91, at 8–10.

15. Javier Pallero & Veronica Arroyo, *Your Data Used Against You: Reports of Manipulation on WhatsApp Ahead of Brazil's Election*, ACCESSNOW (Oct. 26, 2018), https://www.accessnow.org/your-data-used-against-you-reports-of-manipulation-on-whatsapp-ahead-of-brazils-election/.

16. Many areas are also instead controlled by the FTC, and some states, such as California, have laws that differ from the rest—the Health Insurance Portability and Accountability Act ("HIPAA"), for example, indicates one area that is more protected on a federal level. While there has been talk in Congress of introducing a general federal privacy law, no such law has been implemented at this time. *See* CLARE Y. CHO & KRISTEN E. BUSCH, CONG. RSCH. SERV., R47298, ONLINE CONSUMER DATA COLLECTION AND DATA PRIVACY (2022).

17. Fredric D. Bellamy, *U.S. Data Privacy Laws to Enter New Era in 2023*, REUTERS (Jan. 12, 2023), https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/.

18. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, WIRECUTTER, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of- privacy-laws-in-us/.

and that they are free from worry of their data being breached or being used for purposes that they did not approve of.[19] Legislation with these goals may result in nothing more than a standard assurance on each webpage for consumers, but with an easy-to-access form that could be used to report instances of noncompliance (and many examples of the enforcing body actually following through with such reports).

With the increase in smart devices tracking and registering all sorts of data, sensitive or not, it is only rational that there would also be an increase in the push for improved data privacy legislation intended to protect users.[20] The EU's data privacy laws could be seen as the start of that push, but whether the rest of the world follows remains an open question.

This comment will argue in favor of stricter data protection laws in the US and internationally by analyzing the current state of such laws in the US and EU, what measures could reasonably be taken to improve the data protection policies in the US, and what impact those would have on the average user. After all, extensive data protection laws are in the best interests of consumers as well as the companies that the restrictions apply to, even if it may take a bit of adjustment from the status quo.

D. The Legal Landscape of Data Privacy in the EU and the US

The following section will give an overview of the GDPR, the impact the GDPR has on the US, and the status of data privacy legislation in the US.[21]

---

19. *Id.*

20. One may ask, if the average user's typical experience with a violation of data privacy is merely more over-specified ads, then why does it matter? On an individual level, there is no denying that the argument for data privacy varies wildly in how compelling it can be. If someone does not care that their information is being bought and sold to sell them products that an algorithm thinks align more closely with their interests, what can be done to convince them that it is a problem? This issue could once again be rooted in the novelty of the field; once people become even more entrenched in the Internet, their online selves, and the things they use 'smart' devices for, the rules developing now could have even greater implications. *See generally, id.*

21. For the purposes of this comment, I will primarily be focusing on the laws of the US and the EU, as they present some of the more recent and clearly set out regulations in place surrounding data privacy. However, this is not to say that other countries do not have data privacy concerns or legislation, nor that those laws are not also wide-reaching.

1. The GDPR: The Future is Here, and it is Mostly an Improvement

In 2018, the EU put the General Data Privacy Regulation into effect.[22] The GDPR is one of the strictest regulations on data privacy in the world, and its rules are imposed not just on those from and within the EU, but also on businesses and countries that have interactions with EU citizens—for example, American platforms that have users within the EU's domain.[23] For those affected, the rules impose higher standards of transparency and care in relation to the data of consumers.[24] The system of imposing fines is extensive, with variations depending on the severity of the breach and the level of negligence (or malice) needed in order for such a breach to occur.[25] Companies that violate the GDPR's terms can be given a temporary or permanent ban, fines of twenty million euros or four percent of "total worldwide turnover,"[26] or both, depending on the circumstances.[27]

See Craig Riddell, *International Data Privacy Laws: A Guide*, NETWRIX (Sept. 18, 2023), https://blog.netwrix.com/2023/09/18/ international-data-privacy-laws/.

22. Although the GDPR was adopted in 2016, it was not put into effect for two years to allow the affected businesses to adapt to its policies prior to the effective date. *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 99, General Data Protection Regulation, 2016 O.J. (L 119) 1 [hereinafter GDPR].

23. Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr/ (last visited Nov. 25, 2023).

24. The GDPR declares that the data of consumers be processed "lawfully, fairly, and in a transparent manner," and dictates that collection be limited only to what is absolutely necessary. It also mandates that affected companies monitor the data they collect and alert consumers of a breach as quickly as possible, among other things. *See* GDPR, *supra* note 22, art. 5.

25. For example, if a data breach was caused due to a small error from one low-level employee, the fine imposed would be far less than if the breach was caused due to the alleged negligence of many upper-level employees. *See* Paul Nemitz, *Fines Under the GDPR*, *in* 11 DATA PROT. & PRIV.: THE INTERNET OF BODIES 231, 241 (Ronald Leenes et al. eds., 2023).

26. Total worldwide turnover is a synonym for a company's total revenues over some period of time. *See* Adam Hayes, *Overall Turnover: What it Means, How it Works*, INVESTOPEDIA (Jan. 26, 2023), https://www.investopedia.com/terms/o/overall-turnover.asp.

27. *Top Five Concerns with GDPR Compliance*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance (last visited Nov. 25, 2023).

Despite the hefty fines and lofty possible consequences, given the stringent standards applied, some companies have had difficulty adapting to the new rules.[28] Nonetheless, in the years since the regulation's imposition, it is possible that other factors have led to increased compliance. Although the maximum fines and other punishments have rarely been enforced, the modern-day transparency and publicity of data breaches and misuse poses a potential threat of public backlash.[29] The risk to one's reputation or loss of prospective profits from a sudden lack of public goodwill in the case of a violation may have presented enough possible consequence in and of itself to push businesses to exercise greater care and compliance.

Moreover, adoption of the GDPR was not perfectly smooth across the international stage as it resulted in the need for new agreements with the US and other countries.[30] One of the most recent developments, in 2022, was the passing of the Digital Services Act ("DSA"), which increased the number of regulations to be imposed on platforms in the EU's domain in order to prioritize the data privacy and protection of its citizens.[31] Many of the rules in the DSA are set in opposition to the common practices of international companies, like Amazon and Facebook, which must change their behavior and policies regarding consumer data to continue operating within the bounds of the

28. *Id.*

29. Alison Berryman, *GDPR Fines: Are They Working?*, INFOSECURITY MAG. (May 25, 2023), https://www.infosecurity-magazine.com/opinions/gdpr-fines-working/.

30. The EU's adequacy decisions regarding data privacy apply to all foreign governments—including the US—which have had to change their laws to meet the EU's standards. *See* Jennifer Wu & Martin Hayward, *International Impact of the GDPR Felt Five Years On*, PINSENT MASONS (May 25, 2023), https://www.pinsentmasons.com/out-law/analysis/international-impact-of-the-gdpr-felt-five-years-on; *See Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows*, EUR. COMM'N (July 10, 2023) [hereinafter EU TADPF Release], https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 (describing how the GDPR requires other countries' data privacy laws to meet certain standards with respect to how they use EU citizens' data).

31. These new rules dictate what is and is not allowed on these digital platforms, as well as advocate for an increase in transparency in what is done with the data they collect from consumers. 2022 O.J. (L 277) 1 [hereinafter Digital Services Act]; *Questions and Answers: Digital Services Act*, EUR. COMM'N (Apr. 25, 2023), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348.

EU.[32] This has been met with both compliance and pushback from the American companies the law envelops, with Amazon in particular arguing that it was being unfairly targeted.[33] Despite that, there has largely been compliance across the board.[34]

Overall, the EU's new data privacy laws set out greater protections for users with an emphasis on providing a more straightforward way to hold platforms accountable.[35] They do so by: banning targeted ads directed towards specific groups, forcing widespread improvements of transparency in how data is used by companies and governments under the law's purview, and providing a way for users to complain to the platform or to their country's government regarding possible breaches and how to seek compensation.[36] The GDPR also contains provisions allowing for data collection by researchers, who may be interested in using the data of constituents not for financial gain but in the pursuit of knowledge and a greater understanding of how branches of the Internet operate.[37]

The EU's new data privacy regulations only mandate those changes within the EU itself, as the EU cannot have full control over the Internet as a global entity. Despite this, given the large number of users who are covered by the GDPR, and the general diplomatic pull that the EU has, similar laws with the purpose of protecting users' data may be introduced elsewhere.[38] Additionally, the efficiency of using two separate systems to handle user data—one for those affected by the EU's laws and one for those not bound by them—may increase operating costs for

32. Clothilde Goujard, *Facebook, Twitter to Face New EU Content Rules by August 25*, POLITICO (Apr. 25, 2023), https://www.politico.eu/article/facebook-twitter-to-face-new-eu-content-rules-by-august-25/.

33. Clothilde Goujard, *Big Tech Firms First in Line for Fines Under the EU's Content Law*, POLITICO (Aug. 24, 2023), https://www.politico.eu/article/dsa-x-twitter-facebook-meta-snapchat- tiktok-google-instagram-content-law/.

34. *See id.* (describing how Amazon was the only major corporation that attempted to dispute the law, but even then, it eventually said it would comply).

35. Digital Services Act, *supra* note 31.

36. *Id.*

37. *Id.*

38. *See* Chris Velazco, *What the E.U.'s Sweeping Rules for Big Tech Mean for Your Life Online*, WASH. POST (Aug. 30, 2023), https://www.washingtonpost.com/technology/2023/08/30/eu-digital-services-act-faq/ (describing the impact of the GDPR outside of the EU).

companies to the extent that it would be easier to simply have the same policies across the board.[39]

2. The Spreading Legislative Impact of the GDPR on the United States

The chain reaction described above may have already caught on in the US. The Transatlantic Data Privacy Framework ("TADPF" or "Framework"), the result of a 2022 executive order, provides both greater protections for the data of American users and rules for how the protected data of EU constituents can and cannot be used.[40] If one must treat the data of foreigners with a certain level of care, and if it is particularly difficult to distinguish the data of different users, then the TADPF may be the first of many laws paving the way for greater data privacy for Americans. In addition to that, the Framework provides a mechanism for redress of grievances for international users who feel that their data privacy has been violated by an American company or user.[41] Depending on the extent and severity of these claims, the mere existence of this redress mechanism may encourage platforms to treat all consumers' data with more care regarding privacy.

The TADPF arose, at least in part, because the EU declared the US' regulation of the data of its citizens and foreigners to be inadequate, particularly due to surveillance concerns.[42] Following that, it was necessary for the US to amend its existing laws, as under the GDPR it would be illegal for companies in the EU to transfer user data to the US.[43] Discussions of the TADPF's effects

---

39. *Id.*

40. EU TADPF Release, *supra* note 30; *FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, THE WHITE HOUSE (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

41. The framework was set out by Executive Order 14,086; it seeks to facilitate data transfers across borders and also decrees that data transferred from the EU must be met with an "adequate level" of data protection. *See* Exec. Order No. 14,086, *supra* note 14; *see also* EU TADPF Release, *supra* note 30.

42. *See* EU TADPF Release, *supra* note 30.

43. The declaration was made in an EU case referred to as *Schrems II*, which focused heavily on the implications of US surveillance laws, such as Section 702 of FISA. *See* Wu & Hayward, *supra* note 30.

center around the ease of maintaining business in technology while ensuring that US companies comply with the rules set in place in the EU.[44] The US' position is not unique to this agreement as the GDPR mandates that all countries involved in business in the EU give its citizens an "adequate level of protection," thus, the negotiations resulting in the TADPF are a testament to how powerful that mandate can be.[45] Another major concern addressed by the Framework is the prevalence of American intelligence surveillance of international data. While the Framework does provide additional protections, American citizens still face uncertainty over how the US has treated their data in the past.[46]

3. The Abysmal State of Data Privacy in the States: Over-Surveillance

One of the major concerns as to how the US government handles and treats data privacy, and how that may be a danger to international actors and citizens, is clearly illustrated with Section 702 of FISA. Section 702 is used by the United States government to intercept data from any citizen who has had digital communications with a non-citizen abroad.[47] Arguments for data privacy and against this law are often supported by the Fourth Amendment's protections for Americans against "unreasonable searches and seizures," and the Supreme Court has held that encroachment on a reasonable expectation of privacy falls under that protection.[48] FISA and Section 702 allow searches of data without a warrant, regardless of the basis for the search.[49]

---

44. Wu & Hayward, *supra* note 30; THE WHITE HOUSE, *supra* note 40.

45. GDPR, *supra* note 22, ¶ 103.

46. *See generally* EU TADPF Release, *supra* note 30; *see also* Elizabeth Goitein, *The Coming Fight Over American Surveillance*, FOREIGN AFFS. (June 6, 2023), https://www.foreignaffairs.com/united-states/coming-fight-over-american-surveillance (establishing that the United States government has used certain intelligence laws, such as Section 702 of FISA, to impose wide-reaching surveillance measures for both citizens and those abroad).

47. Charlie Savage, *Security Agencies and Congress Brace for Fight Over Expiring Surveillance Law*, N.Y. TIMES (Feb. 27, 2023), https://www.nytimes.com/article/warrant less-surveillance-section-702.html.

48. Goitein, *supra* note 46.

49. *Id.*

Officials tout Section 702's usefulness in combatting cyber-attacks, drug trafficking, and espionage; however, it has also caused issues with privacy agreements abroad, notably with the EU, and was one of the factors leading to the need for the TADPF.[50] That is due to Section 702 allowing surveillance based merely on the transmission of any "information related to the conduct of U.S. foreign affairs."[51] This broad definition allows for data collection of both citizens and non-citizens, and can have threats not just to the privacy of the individuals involved, but give rise to civil rights issues.[52]

III. THE IMPACT OF THE EU'S DATA PRIVACY LEGISLATION, AND WHY THE WORLD MUST FOLLOW SUIT

A. The Benefits of More Extensive Data Privacy Laws

The EU's GDPR provides the clearest picture of the realistic implications of a strict data privacy law system, as it has been around long enough to see what, if any, impacts it has had on its users, consumers, and businesses. The consumer benefits of the GDPR include the right to data protection, which is included in the EU charter of fundamental rights. This right to data protection can influence other rights such as freedom of speech, thought, or assembly by ensuring users are free to act and speak as they wish online.[53] Other rights include preventing fraud and making it easier for consumers to see what is done with the information and data that they put out onto the Internet.[54]

---

50. *See* OFF. DIR. NAT'L INTEL., SECTION 702 OVERVIEW 1–2 (2023) (presenting an overview of the law from the perspective of the Office of the Director of National Intelligence, which prioritizes surveillance as a matter of safety); *see also* EU TADPF Release, *supra* note 30.

51. Goitein, *supra* note 46.

52. For example, in 2020, the Department of Homeland Security monitored the social media accounts of people protesting for racial justice, and it was also reported that the Department of Defense had purchased geolocation data from popular Muslim prayer and dating apps. Additionally, in 2022, social media accounts were monitored for "reactions" about the *Dobbs* decision. These incidents demonstrate that warrants and data privacy protections work not only to protect privacy, but also civil rights. *See id.*

53. *Data Protection Benefits for You*, EUR. DATA PROT. BD., https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-benefits-for-you_en (last visited Mar. 4, 2024).

54. *Id.*

These opt-in models, where the consumer must make a choice to allow their data to be used and the restrictive option is the default, for consumers' consent to sharing their data do not necessarily mean that there is a decrease in data gathered. In fact, one study found that the opposite was true—there were slightly more consumers sharing more data than before.[55] Even though the company in charge of a given website receives less data from its userbase with those opt-in data sharing options chosen, that same study (surrounding a large telecommunications provider in Europe) showed that the opt-in model allowed the business to increase its profits.[56] The reason for this may be that consumers find companies that provide an option to share less data (sensitive or otherwise) to be more trustworthy, and are more likely to choose it over a service that does not provide that option.[57] The study also shows increased profits from consumers who allowed greater use of their data.[58] Even though those who opt-in to increased restrictions on the use of their data are less likely to be marketed to, this indicates that those who choose to opt-out of the increased restrictions are also those who would be more receptive to targeted advertising.[59] In other words, with the ability to opt-in or out of the use of data, all groups involved see some sort of benefit: those consumers who do not want their data used or to be shown targeted ads can have that, consumers who do not mind targeted ads continue to see them, and the corporations in charge are only able to market towards a base of consumers likely to consume their product.[60]

Even though the results of that specific study may not exactly be replicable in every field that utilizes targeted ads, the impact it would have on the consumer base is obvious (particularly concerning targeted advertisements, which some find

55. Miguel Godinho de Matos & Idris Adjerid, *Consumer Consent and Firm Targeting after GDPR: The Case of a Large Telecom Provider*, MGMT. SCI., July 2019, at 4.

56. *Id.* at 5.

57. *See id.* at 3 (describing evidence that indicates that better privacy protections can make consumers trust the companies in charge of that data more than they would have otherwise).

58. *Id.* at 5.

59. *Id.* at 27.

60. *Id.*

unsettling).[61] Despite this, it would be difficult to get rid of entirely, as digital advertising, including targeted ads, has become a fundamental part of how the Internet functions.[62] Targeted ads, while providing somewhat more relevant products to possible consumers, are not overwhelmingly better at providing good results or a variety of options in comparison to a potential consumer searching for an item themselves, particularly with the presence of "low-quality vendors."[63] However, given that the Internet, and a large chunk of the global economy, is so dependent on advertising—targeted or otherwise—removing advertisements entirely is likely out of the question. Due to the prevalence of the Internet, the best option is to follow in the footsteps of those countries that have provided increased measures of consent and transparency in consumer data to improve the well-being of the market. As the study above demonstrated, given the option, not everyone will opt-in to increased protections.[64]

What exactly qualifies as targeted advertising, identifiable data, or anything else that the GDPR aims to protect is unclear. While the regulation is extensive, it neglects to define targeted advertising.[65] One way to think about targeted advertising is that it functions as a means of identifying a consumer (e.g., a service may come to know a user's name, place of residence, or age so as to target advertising towards them).[66] Code itself, if it pertains to

61. *See* Brian X. Chen, *Are Targeted Ads Stalking You? Here's How to Make Them Stop*, N.Y. TIMES (Aug. 15, 2018), https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html (describing one common experience of consumers with targeted ads looking up a specific product and then seeing advertisements for similar products).

62. EDUARDO ABRAHAM SCHNADOWER MUSTRI, IDRIS ADJERID, & ALESSANDRO ACQUISTI, BEHAVIORAL ADVERTISING AND CONSUMER WELFARE: AN EMPIRICAL INVESTIGATION (2022).

63. The study concludes by saying that the increased use of adblockers makes it more difficult for "high-quality vendors" to reach consumers and that this is a downside for consumers. This may be true, but here a new question is raised: Does a consumer really *need* to buy a product, or is this something that only matters for the vendor themselves? *See id.* at 22.

64. *Id.* at 17.

65. Nadezhda Purtova, *From Knowing by Name to Targeting: The Meaning of Identification Under the GDPR*, 12 INT'L DATA PRIV. L. 163, 173 (2022).

66. *See id.* at 166. Notably, "the GDPR does not directly define identification" either, although its definition of personal data can be indirectly relied upon to do so and to

users at all, may even be considered personal data under the GDPR. While code hasn't been the subject of much litigation, if it does arise and is confirmed to be included under the "personal data" umbrella, such a decision could have wide-ranging effects due to the scope of users who design or use code in their daily lives.[67]

1. Users in Control? Public Attitudes Towards Data Privacy

Putting control of data into the hands of consumers is a logical step in seeing the Internet as less of a commodity and more of a necessity; it also more easily allows consumers to hold vendors and businesses accountable if something goes wrong. The GDPR and other agreements are simply the groundwork for the future. As the Internet continues to expand in its current and potential uses, it is essential to ensure the protection of the rights of people using platforms, buying products, or generally existing in a digital space. Most consumers in the US and abroad care about data privacy and would take some additional measures to protect their data;[68] as a result, data privacy legislation is something that most people care about and would probably like to see expanded. Assuming those attitudes continue as people share more of their lives online, some suggest that the future may lead to a decrease in (or elimination of) tracking entirely, or the potential for incentives to be offered to consumers for giving their data to vendors.[69] This future is even more likely if laws similar to the

---

subsequently distinguish targeting as a method by which an individual is selected out of a group they belong to as "an object of attention or treatment in a single moment of time."

67. Nadezhda Purtova & Ronald Leenes, *Code as Personal Data: Implications for Data Protection Law and Regulation of Algorithms*, 13 INT'L DATA PRIV. L. 245, 246 (2023).

68. In a 2023 study with respondents from twelve countries (including the US and four EU member-states), 87% answered that they cared about their data. *See* CISCO, GENERATION PRIVACY: YOUNG CONSUMERS LEADING THE WAY: CISCO 2023 CONSUMER PRIVACY SURVEY 5 (2023); *see also* Robert Waitman, *Generation Privacy*, CISCO BLOGS (Oct. 18, 2023), https://blogs.cisco.com/security/generation-privacy (summarizing the study's findings and providing its publication date).

69. Even in a future with "no tracking," given how heavily the Internet relies on advertising, it's unlikely that targeted ads will cease to exist entirely. Those who opt-in (or those who forget or neglect to opt-out) will likely still be subjected to targeted ads unless

GDPR are put into effect elsewhere, or if the GDPR expands its influence through further international agreements.

The benefits of a system of stricter data privacy laws are more evident for governments than private entities. As previously mentioned, the US has been known to use the data of its citizens for surveillance, without needing to provide much justification in that process.[70] Without protections in place, citizens are being unknowingly subjected to overbearing and unreasonable processes, creating the opportunity for them to be targeted for additional surveillance due to characteristics such as their political views, race, or religion.[71] The allowance of such collection in the name of surveillance is ethically objectionable, and the use of data for surveillance needs to, at the very least, be heavily regulated to prevent such behavior.

B. The GDPR and the US: its Impact, Implications, and Issues

To see what further implications of the GDPR may be for businesses in the US (as well as potential legislation), it is important to compare the GDPR with the existing state laws regarding data privacy. One important difference between the GDPR and at least three of the earliest enacted state privacy laws (in California, Virginia, and Colorado) is that the GDPR operates on an opt-in basis whereas the state laws operate on an opt-out basis (the opposite process of the opt-in model).[72] The GDPR also has more extensive fines and consequences for those in breach of the agreement.[73] The discrepancies between the GDPR and the state-level laws may cause difficulties for companies looking to operate in both markets, such as needing to expend more

there is an outright international ban on the practice. *See* Swish Goswami, *What the Future of Consumer Data Ownership Looks Like*, FORBES (Nov. 23, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/11/23/what-the-future-of-consumer-data-ownership-looks-like.

70. Goitein, *supra* note 46.

71. *See* Goitein, *supra* note 46 and accompanying text (illustrating how the US government has used user data in the past to target such groups).

72. *Comparing U.S. State Data Privacy Laws vs. the EU's GDPR*, BLOOMBERG L. (July 11, 2023) [hereinafter Privacy Law Chart], https://pro.bloomberglaw.com/brief/privacy-laws-us-vs-eu-gdpr/.

73. *Id.*

resources to ensure compliance or creating diplomatic disagreements and further legislation.[74]

As far as impacts on consumers and producers in the US, the GDPR's influence is already apparent. The EU was able to influence the US into enacting the TADPF, and the GDPR has been in effect for a couple of years already, with many companies changing how they behave online in order to comply.[75] This has not been without its hiccups, however. On average, the cost for companies to implement policies complying with the GDPR is estimated to be 16 million dollars.[76] Some businesses have attempted to avoid the GDPR by physically changing the location of the data stored for their EU users; for example, both Facebook and Google have moved users and their relevant servers away from GDPR jurisdictions.[77] Even though those two corporations may be outliers, having the vast resources and ability to undertake such a task to avoid the GDPR, Google and Facebook are two of the most used websites on the Internet with billions of users, making a large profit through advertising sales based on user data.[78] Their duty regarding the data privacy of users should not be able to be skirted simply by changing the location of the

74. The latter has already been observed via the US being forced to enact the TADPF, which would not have been put into effect without the EU's insistence upon better data protection laws for its citizens' data in the US. *See* EU TADPF Release, *supra* note 30.

75. Goujard, *supra* note 32; *see also* Goujard, *supra* note 33 (describing the requirements for compliance with the GDPR and the fees for breach, and how these have resulted in changes to policies in order to foster compliance).

76. Mona Naomi Lintvedt, *Putting a Price on Data Protection Infringement*, 12 INT'L DATA PRIV. L. 1, 4 (2022).

77. *See id.* (citing news articles discussing these corporations moving their users away from the GDPR's jurisdiction).

78. Google, one of the first websites many users use any time they access the Internet, has billions of users for its apps alone. Facebook has almost three billion users for its large family of apps that operate in a similar method to Google's. *See* Matt Burgess, *All the Data Google's Apps Collect About You and How to Stop It*, WIRED (Apr. 5, 2021), https://www.wired.co.uk/article/google-app-gmail-chrome-data (describing how Google collects data from each of its apps and what it sells that data for); Hemant Shama, *Facebook Users Statistics and Trends: How Many People Use Facebook in 2024?*, ADSCHOOLMASTER (Feb. 14, 2024), https://www.adschoolmaster.com/ facebook-users-statistics/.

data—which is one reason why the TADPF, and any subsequent legislation, is so important.[79]

1. What Has Made the GDPR So Effective?

Even though the GDPR is only directed at protecting all users within the EU's territorial sphere (regardless of residency), that does not mean that the law as it stands has no impact on businesses located outside of the EU.[80] The law has a direct impact on companies that have operations of any kind in the EU, and imposes its standards of data privacy and accountability onto foreign companies that wish to continue operating within the EU.[81]

The success of the GDPR can, in part, be attributed to its allowance of large fines for violations.[82] However, while the practice of fines is one of GDPR's greatest strengths, it also highlights a key weakness of the regulation: the lack of consistency in enforcement between EU member countries.[83] While the cumulative total of fines imposed for GDPR violations has reached well over 5.6 billion euros (as of February 2025), over half of that amount (3.5 billion) are fines imposed by Ireland alone, despite the country only issuing 30 fines.[84] In contrast, Spain has filed 916 fines which have only totaled 88.3 million euros—Italy is in second place for total number of fines imposed,

79. These concerns have been the subject of laws proposed to Congress. However, there have been no expansive, federal laws passed regarding data privacy. *See* Gregory T. Parks & Ronald W. Del Sesto, Jr., *US Data Privacy Legislation: Could a Federal Law be on the Horizon?*, MORGAN LEWIS (July 31, 2023), https://www.morganlewis.com/pubs/2023/07/us-data-privacy-legislation-could-a-federal-law-be-on-the-horizon.

80. For the purposes of this comment, I will be focusing specifically on those businesses operating in the US. *See* Yaki Faitelson, *Yes, The GDPR Will Affect Your U.S.-Based Business,* FORBES (Dec. 4, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/.

81. *Id.*

82. Lintvedt, *supra* note 76, at 2.

83. *Id.* at 5.

84. *See* Fines Statistics, GDPR ENFORCEMENT TRACKER, https://www.enforcementtracker.com/?insights (last visited Feb. 13, 2023). This describes the breakdown of GDPR enforcement by country, the number of fines given out, and how much each country has imposed as a fine as of February 2025. It is important to note, however, that the database addresses only which fines are publicly listed, and there could be more fines that are not visible to the public.

with 396.[85] The data above demonstrates that even though all of the member countries are under the jurisdiction of the GDPR, that does not necessarily mean that each enforces the law and imposes its fines in the same way, as frequently, or with as much force as its neighbors. The highest fines have been for major platforms such as Meta, Amazon, TikTok, WhatsApp, and Google, and have only been enforced in certain countries.[86] It is highly possible that the behaviors resulting in fines in certain countries were overlooked and not enforced by a fine in others. As a result, the overall compliance with the law by major platforms may be less cohesive than it appears. For example, Spain seems to enforce and fine based on violations from smaller businesses and private individuals far more often than Ireland, which has primarily imposed fines to major foreign-based platforms as well as major Irish institutions, such as its Department of Health.[87]

2. The TADPF as a Measure of the GDPR's Impact in the United States

On a diplomatic level, the GDPR's influence has already become evident with the enactment of the TADPF.[88] The TADPF is not even the first such law to exist for its purpose between the EU and United States; the law before TADPF was declared inadequate (primarily due to surveillance concerns) and TADPF was drafted with those criticisms in mind.[89] If further challenges arise regarding the suitability of US data privacy laws as to how they treat EU consumers' data, it is not out of the question that more expansive legislation could be promulgated. In a broader sense, if the GDPR was able to push the US to introduce a new law in compliance with the regulations, it is also likely that the

85. *Id.*

86. *Id.*

87. *Id.*

88. *See* EU TADPF Release, *supra* note 30 (describing how the EU caused the US to create new laws by deeming its existing law for EU citizens' data unacceptable).

89. CHRIS D. LINEBAUGH & EDWARD C. LIU, CONG. RSCH. SERV., R46724, EU DATA TRANSFER REQUIREMENTS AND U.S. INTELLIGENCE LAWS: UNDERSTANDING SCHREMS II AND ITS IMPACT ON THE EU-U.S. PRIVACY SHIELD 5–7 (2021) (giving an overview of *Schrems II*, the case which found the existing law, the EU-US Privacy Shield, to be inadequate).

EU could advocate for similar legislation in other countries.[90] In the US alone, however, the GDPR may influence the state-level data privacy laws to bring them closer to the standards of protection in the GDPR, or even have some weight if a comprehensive federal privacy law is created. Given the already apparent influence, it is highly possible that the EU could use the success it has seen with the GDPR to persuade lawmakers to enact stricter privacy laws.

The GDPR has already emerged in a few court cases in the US: from small claims addressing data breaches that happened to impact EU users,[91] to major claims against Facebook and Google. While the GDPR concerns in the cases against Facebook and Google were mere mentions in major securities claims regarding severe data breaches, the evidence presented makes it clear that such corporations were concerned about how the foreign law would impact them.[92] Two cases in particular address, at least in part, a direct claim brought by parties regarding data breaches:[93] one brought in New York based on the UK's GDPR

90. Many countries (such as South Africa, Ghana, China, and Australia) have existing data privacy laws that do not exactly align with the GDPR, and they may need to create new standards if these laws are found to be inadequate, as demonstrated by the situation that led to the creation of the TADPF in the US. As another testament to its influence, the GDPR has already served as a model for many other countries in drafting their own data privacy laws. *See* Wu & Hayward, *supra* note 30.

91. *See* In re Mercedes-Benz Emissions Litigation, 2020 WL 487288, at *8 (D.N.J. Jan. 30, 2020) (affirming the plaintiffs may obtain the discovery they are entitled to pursuant to the Federal Rules of Civil Procedure while protecting EU citizens' private data pursuant to the GDPR).

92. *See In re* Facebook, Inc. Sec. Litig., 84 F.4th 934, 946 (9th Cir. 2023) (describing how Facebook attributed low revenue growth and a decline in users across Europe to "putting privacy first" in its implementation of the GDPR); *see also In re* Alphabet, Inc. Sec. Litig., 1 F.4th 687, 708 (9th Cir. 2021) (describing how both Google LLC and Alphabet, Inc. took the GDPR into account when internally analyzing their major data breaches).

93. It is also important to note that while neither case was dismissed outright for lack of standing, the *Finch* court did not find compelling reason for the case to be brought in New York court, and the *Katz-Lacabe* case primarily concerned the claims brought by the American members of the plaintiff's party—the single GDPR violation claim was not given substantial weight. These both demonstrate that, in order to have standing and actually be enforced, a similar claim would need a substantial amount of justification. *See* Finch v. Xandr, Inc., No. 21 CIV. 5964 (VM), 2021 WL 5910071, at *3 (S.D.N.Y. Dec. 14, 2021); Katz-Lacabe v. Oracle America, Inc., 668 F.Supp.3d 928, 949 (N.D. Cal. 2023).

was dismissed due to the irrelevance of the forum,[94] and another brought in California had its GDPR-based claim dismissed due to lack of evidence.[95] These examples illustrate the difficulty in bringing data privacy claims in US court for foreigners, and as such, point in favor of the TADPF's new systems. Alternatively, the dismissal of these cases indicates that the process for bringing claims against American companies under the GDPR and similar policies needed revision for certain scenarios and could benefit from the clarification that the TADPF provided. Particularly in the situation in *Katz-Lacabe*, when the plaintiffs are comprised of a mixture of US and EU citizens and the claim has standing, what remedy would be available for the class as a whole? The answer is not clear, but one thing is: such claims would, at least in theory, have an easier time being brought in the US under the system the TADPF created for claiming a breach of the standards imposed by the GDPR.

However, the redress system established by the TADPF, including the establishment of a dedicated court for such claims, is not without its flaws. How much help it will be—and has been—for the average person is unclear. The process appears to be long, with a lot of discourse between governments, resulting in a response from the United States that does not specify whether there was a violation or not.[96] Similarities have been drawn between the current system of redress and the one created for the privacy agreement that existed prior to the TADPF, with focus on

94. While the U.K.'s GDPR is not the same as the EU's—notably in that the GDPR for the EU mandates that claims be brought in EU courts—this can stand as an interesting precedent for cases brought in US court for such data privacy claims. It is also notable that this case was decided before the TADPF was enacted. Now, with the new agreements, it is possible that a similar claim made under the EU rather than the U.K. laws could survive through the process that the TADPF specifically sets out. *See* Finch v. Xandr, Inc., 2021 WL 5910071, at *4.

95. Here, the court pointed to significant differences between California law and the GDPR and came to the result that an "intrusion upon seclusion" claim could not stand without an explanation of additional evidence that could be produced by discovery. *See Katz-Lacabe*, 668 F.Supp.3d at 949.

96. Alfred Ng & John Sakellariadis, *Inside Biden's Secret Surveillance Court*, POLITICO, https://www.politico.com/news/2024/01/17/inside-bidens-secret-surveillance-court-00136175 (last updated Jan. 18, 2024).

its lack of transparency and usefulness for EU and US citizens.[97] If those similarities become strong enough, it could lead to issues for the TADPF as a whole similar to those in the deciding case that led to its creation.[98]

3. A Coming Storm for the TADPF?

There is no guarantee that the TADPF will last in its current state forever. The EU scheduled a review of the TADPF's functionality in July 2024, and continuing reviews will occur at intervals of, at most, every four years.[99] The same organization involved in the case in which the EU decided the existing agreement was inadequate has already made clear its intention to challenge the TADPF; such a challenge, if successful, could result in an entirely new agreement (not unlike the process that resulted in the framework itself).[100] The lack of stability indicates that the TADPF is not an entirely permanent solution, but one that was brought out of necessity, and may need to be changed in the future to fulfill its purpose in entirety. Some of the arguments against TADPF's adequacy may surround the justification of data collection by US intelligence agencies, as well as bulk collection of data.[101] The former concern intersects with those brought by Section 702, as addressed above; what can be considered adequate when collecting data from such a broad range of people, for any kind of reason?[102] Bulk data collection falls under a similar concern, but, rather than targeting a specific person, a

97. These criticisms are being raised, in part, by Max Schrems, an advocate for privacy who initiated the lawsuit that sparked the creation of the TADPF itself. *See id.*

98. C-311/18, Data Protection Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, ECLI:EU:C:2019:1145 (2020), *available at* http://curia.europa.eu/juris/liste.jsf?num=C-311/18.

99. Rohan Massey & Christopher Foo, *New EU-US Data Privacy Framework – Key Takeaways for Transatlantic Data Transfers*, ROPES & GRAY (July 12, 2023), https://www.ropesgray.com/ en/insights/viewpoints/102ij4x/new-eu-us-data-privacy-framework-key-takeaways-for-transatlantic-data-transfers.

100. *Id.*

101. Mikołaj Barczentewicz, *Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States*, INT'L CTR. FOR L. & ECON. (Sept. 25, 2023), https://laweconcenter.org/resources/schrems-iii-gauging-the-validity-of-the-gdpr-adequacy-decision-for-the-united-states/.

102. *See* Goitein, *supra* note 46 (describing the extensive data collection and use justified by Section 702).

government collects mass amounts of data from an incredibly large group.[103] These kinds of concerns must be addressed not only in agreements with the EU, but also in data privacy laws within the US. To do so would require a reckoning of sorts within the US government to decide what matters more: the right to privacy of its citizens or an overbearing policy in the name of national security.[104] Taking that into consideration, in the coming section I will address: what a law in the same vein as the GDPR would look like in the US; how effective that could be; how it could be different, or even better, from the GDPR as it exists in the EU; and other potential impacts.

C. *An American GDPR: Federal Legislation, Speculation, and Existing State Laws as a Roadmap*

For some in the US, strong data privacy laws are not so difficult to imagine. While there is no overarching federal law regarding data privacy, some states have taken matters into their own hands. As of 2023, thirteen states have enacted comprehensive consumer privacy laws, and many others have more specific legislation (for example, laws regulating privacy for children on the Internet).[105] Even among those states with comprehensive agreements, however, the laws are not always the same. For example, the law enacted in Texas in 2023 (effective July 1, 2024) exempts certain categories of advertisers from necessarily needing to comply with the legislation, grouping it with the category of state laws that are considered more "business-friendly."[106] However, despite the variations between

103. One notable example of this is the data collection that was leaked by Snowden in 2013. While the Act that allowed that bulk collection was modified, it still allows for bulk metadata collection, particularly from phones. *See* Sarah St. Vincent, *Congress Should End Massive Phone Records Spying*, THE HILL (June 20, 2019), https://thehill.com/opinion/civil-rights/449438-congress-should-end-massive-phone-records-spying/.

104. Bellamy, *supra* note 17 (describing that the US system values security when it comes to data privacy, whereas the EU system views data privacy as a human right).

105. Heather Morton, *2023 Consumer Data Privacy Legislation*, NAT'L CONF. STATE LEGISLATURES (Sept. 28, 2023), https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation.

106. Small businesses are exempted from the law, as well as electric and power companies, political entities, and businesses governed by HIPAA. However, Texas also

each state's comprehensive legislation, having some kind of law is, by default, better than having none at all. Regardless of how strong or weak each state's law is, the presence of different standards for business entities represents a challenge to those looking to act in a diverse market, such as the US. On the consumer side, the variation in standards across state lines may, in the best case, be confusing, and in the worst case, be an increase in frivolous warnings and checkboxes.

A federal GDPR-like law would benefit those living in states with their own data protection laws by making the legislation consistent and would most obviously benefit those in states without such laws. However, with the discrepancies seen in the states that have already enacted comprehensive laws, making one cohesive piece of legislation would likely receive a large amount of pushback.[107] Moreover, given the differences in attitudes towards privacy rights in the EU and the US, as well as the differences between the already-existing state laws and the GDPR, it is safe to assume that any federal-level law would likely take more closely after the legislation already existing in certain states.[108] A GDPR for the US would likely be an opt-out model, focus only on residents of the US, and have exclusions for certain types of information and businesses.[109] Given that the states' laws do not have the drastic punishments of the GDPR, a federal data privacy law would likely follow suit.[110] If that is to be the case, however, it is also likely that there will be issues with compliance. One of the main reasons that the GDPR was so notable was because of its large fees for noncompliance, and without that, it is

---

requires additional notice to the consumer if sensitive data may be sold, and it has a requirement for recognition of "universal opt-out mechanisms" for personal data sale and targeted advertising. *See* Nancy Libin et al., *Texas Data Privacy and Security Act – An Overview*, DAVID WRIGHT TREMAINE LLP (July 6, 2023), https://www.dwt.com/blogs/privacy—security-law-blog/2023/07/texas-data-privacy-and-security-act-overview.

107. *See* Morton, *supra* note 105 (describing the different policies present in state laws).

108. Privacy Law Chart, *supra* note 72.

109. *See id.* (setting out the differences between the sets of legislation, in which the US laws have more exclusions and are generally less restrictive than the GDPR).

110. For example, while the GDPR has forced compliance with its laws upon even incredibly large corporations by way of its hefty fines (of up to 4% of worldwide revenue), state laws have imposed punishments based on monetary amounts for specific users impacted or have not listed monetary punishments at all. *See id.*

possible that there may not be as widespread compliance as there was (and is) with the GDPR.[111] On the other hand, the less strict standards and exemptions found in the state legislation may be reflected in federal laws, meaning there is not as great a need for strict punishments. Therefore, companies may have more of an incentive to find ways to fit into those loopholes.[112]

At the very least, a general federal data privacy law is essential for consumers and businesses. One must only look at the EU's policies to see why (prior to the GDPR, many countries had differing levels of consequences, and each's individual policies varied in strictness).[113] The GDPR was beneficial because it provided a cohesive system with a consistent set of punishments.[114] A system akin to that in the US would be even more impactful, at least in part because the GDPR, as enacted by each member country, still has significant variations in the frequency and amount imposed by fines for noncompliance.[115] While the best case scenario for end user data protection would be policies as strict as (or even more so than) those found in the EU, given that states would likely have less of a say regarding the enforcement of fines than EU member countries would, a federal law would be incredibly effective. In this scenario, the data privacy law of the US would be equally fined or otherwise punished for the same reasons across the entire US. Given how effective the existence of the GDPR alone has been,[116] it is easy to

111. *See* Goujard, *supra* note 33 (describing the fees and consequences for companies breaching the law and how those consequences have led to compliance across the board, except for some companies who have complained about being singled out (e.g., Amazon)).

112. Privacy Law Chart, *supra* note 72; *see also* Dan Goodin, *Your iOS App May Still be Covertly Tracking You, Despite What Apple Says*, ARSTECHNICA (Apr. 18, 2022), https://arstechnica.com/information-technology/2022/04/a-year-after-apple-enforces-app-tracking-policy-covert-ios-tracking-remains/ (describing how large companies like Apple and Google still can gather data from users through legal loopholes or terms in their user agreements).

113. Lintvedt, *supra* note 76, at 5.

114. *See id.* at 3 (describing that much of the behavioral change observed from corporations in anticipation of the GDPR was due to the imposed fines rather than its rigidity).

115. *See id.* at 5–7 (illustrating how the variations in enforcement between member countries may inhibit the enforcement power of the GDPR overall).

116. Even if fines are not the main factor in why the GDPR has seen such compliance, they are certainly a major one. Other such factors may include fear of

see how such a law could greatly change the global landscape of data privacy policy.

IV. CONCLUSION

While the GDPR and the TADPF are good starting points in the journey toward a thorough system of data privacy laws, they are only that—a start. The state of data privacy laws in the US is abysmal, and only a minority of states have anything resembling comprehensive data privacy legislation. A more comprehensive, strict, and extensive law is a must if the US wants to cooperate with the EU on a technologically compatible level. Online advertising based on data collection is a billion-dollar business and a major part of the Internet's economy.[117] As society's online presence continues to expand, issues concerning online advertising and data collection will become more significant. The EU's concerns and calls for adequate data protections for its citizens are justified, especially considering the US' tendency to violate the data privacy rights of its own citizens as well as foreigners in the name of security.[118] The EU's prioritization of the right to privacy is clearly the right path to follow.

Additionally, it is essential that the US adopt a general data privacy law on a federal level. In the absence of such legislation, each state has free reign to set its own standards, leading to major differences in how user data is treated, as well as additional concerns regarding where each person is located, where the company is located, and where the data itself is stored. If a state where a social media company operates has stricter data privacy laws than its neighbor, there is nothing currently that stops the company from moving its data storage centers elsewhere.[119] On a simpler level, the lack of a comprehensive federal data privacy law puts people at risk who live in states without such laws. While

community retribution or loss of trust, which, especially for smaller entities, would act as a major deterrent to potentially incurring the loss of their userbase. *See id.*

117. Mustri et al., *supra* note 62.

118. *See* Goitein, *supra* note 46 (describing the history of the US' surveillance policies, particularly with respect to Section 702 of FISA and earlier policies).

119. Such behavior has already been observed. For example, as discussed earlier, Facebook and Google opted to relocate their user data to be outside the jurisdiction of the GDPR. *See* Lintvedt, *supra* note 76, at 4.

there may be some level of protection afforded by the federal government in regard to data privacy, it is not stringent enough to apply to most behaviors that would harm normal users. [120]

As technology becomes an even greater part of everyday life, protecting the digital footprints and fingerprints we all leave behind will become even more essential than it is today. The GDPR, while not flawless and certainly not all-encompassing, is an excellent example of a rule that prioritizes data privacy as a right. Such prioritization should become a standard internationally; as the Internet becomes a public space, why should what one does be monitored if they have done nothing wrong? Monetization of such footprints on the Internet is equally objectionable. The Internet is a public space and a forum through which every user should be able to act as they wish without fear of being tracked, having their data collected and sold en masse by advertisers, or being subjected to a constant barrage of targeted ads. The collection of user data by governments and private entities should be subject to the consent of the user and done only to the extent necessary, with appropriate justification. To not operate on such a level or have laws regulating that kind of behavior, is only asking for the problem to worsen in the future.

120. Examples of harmful behaviors include targeted ads and using user data to determine what political group someone belongs to. *See* Goitein, *supra* note 46 and accompanying text (describing how user data was collected regarding specific political issues or membership in specific minority groups).