Brooklyn Law Review

Volume 85
Issue 1 *Symposium: Incitement at 100-and 50-and Today*

Article 10

12-27-2019

"Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation

Katherine M. Wilcox

"Hey Alexa, Do Consumers Really Want More Data Privacy?"

AN ANALYSIS OF THE NEGATIVE EFFECTS OF THE GENERAL DATA PROTECTION REGULATION

INTRODUCTION

"Big Brother is Watching You."[1] For ages, individuals worldwide have questioned and feared how "Big Brother" uses technology to monitor, influence, and control citizens.[2] Are we being watched? Does someone else gain from the exploitation of our personal information? Do ordinary citizens have a say in this process? Though these questions may appear dramatic or dystopian, all of these concerns become increasingly prevalent in "today's digital age."[3] Recent news sources feature articles discussing incessant emails with updated terms and conditions,[4] Mark Zuckerberg's viral Congressional hearing,[5] and people seeing advertisements for items they just recently saw on Google.[6] Accordingly, lawmakers have become increasingly aware and

---

[1] GEORGE ORWELL, 1984 5 (NAL Penguin Inc. 1961) (1949) (emphasis omitted).

[2] *See generally id.* (describing a social science fiction dystopian society where government surveillance is omnipresent).

[3] 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/#7c65ec4055e5 [https://perma.cc/H5Y6-SB5F].

[4] *See, e.g.*, Brian X. Chen, *Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them*, N.Y. TIMES (May 23, 2018), https://www.nytimes.com/2018/05/23/technology/personaltech/what-you-should-look-for-europe-data-law.html [https://perma.cc/4Z3F-SSKQ].

[5] Wall St. Journal Video, *Mark Zuckerberg's Five Hour Face-Off with Congress in Five Minutes*, WALL STREET J. (Apr. 10, 2018), https://www.wsj.com/video/mark-zuckerbergs-five-hour-face-off-with-congress-in-five-minutes/5C7E88ED-A058-4C2F-873D-34E5EFB817F6.html [https://perma.cc/463N-J85X].

[6] Casey Aonso, *There's a Reason Why You Keep Getting Ads for Things You've Talked About but Haven't Actually Searched up Online*, NARCITY (Jan. 5, 2018), https://www.narcity.com/news/theres-a-reason-why-you-keep-getting-ads-for-things-youve-talked-about-but-havent-actually-searched-up-online [https://perma.cc/9LT7-R3MS].

skeptical of how companies monitor and utilize personal data and how to better protect consumers in this process.[7]

Until recently, the European Union (EU) addressed issues of privacy through the Data Protection Directive (DPD), which the EU enacted in 1995,[8] well before the emergence of big data, smartphones, and mass use of the internet.[9] The DPD, a mere legislative guideline,[10] quickly became irrelevant, as it "fail[ed] to address how data is stored, collected, and transferred today."[11] In efforts to drastically update the DPD and guarantee new protections for individual personal data, the EU began drafting a new regulation called the General Data Protection Regulation (GDPR) as early as June 15, 2015.[12] The regulation, however, only recently became effective on May 25, 2018.[13]

Mandating compliance from all twenty-eight EU member states, the GDPR establishes a framework that sets legal standards targeted at businesses and other data collectors to protect the privacy and personal information of the citizens of the EU.[14] Generally, the legislation applies to *any* company that processes the data of individual EU citizens. Thus, the list of affected parties includes technology firms, banks, social media companies, insurance companies, advertisement and marketing services, and financial companies,[15] along with governments and small businesses.[16]

As the first regulation of its kind to provide updated standards and security measures for personal data and privacy, the GDPR greatly impacts businesses operating internationally.[17]

---

[7] *See* Alex Hern, *What Is GDPR and How Will It Affect You?*, GUARDIAN (May 21, 2018), https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you [https://perma.cc/3UNV-HUJ3]; Chen, *supra* note 4; Rossow, *supra* note 3.

[8] Hern, *supra* note 7.

[9] Tripwire Guest Authors, *GDPR – The Good, the Bad, and the Ugly*, TRIPWIRE (Feb. 23, 2016), https://www.tripwire.com/state-of-security/security-awareness/gdpr-the-good-the-bad-and-the-ugly/ [https://perma.cc/85JC-6J9G].

[10] Kyle Petersen, *GDPR: What (And Why) You Need to Know About EU Data Protection Law*, UTAH B.J., July–Aug. 2018, at 12, 12 ("A directive is EU legislation that requires member states to achieve a certain goal but allows each member state to implement its own laws on how to reach such goal.").

[11] Rossow, *supra* note 3.

[12] *See* Jan Philip Albrecht, *Foreword: How the GDPR Will Change the World*, 2 EUR. DATA PROTECTION L. REV. 287, 287 (2016); *Timeline of Events*, EU GDPR, https://eugdpr.org/the-process/timeline-of-events/ [https://perma.cc/2ND2-L3Q3].

[13] Hern, *supra* note 7.

[14] Rossow, *supra* note 3.

[15] *See* Susan Akbarpour, *How Does GDPR Impact Advertising and E-Commerce?*, FORBES (May 8, 2018, 9:00 AM), https://www.forbes.com/sites/forbesagencycouncil/2018/05/08/how-does-gdpr-impact-advertising-and-e-commerce/#4dbb05ba3277 [https://perma.cc/BM5E-RPFF]; Rossow, *supra* note 3.

[16] Che Kohler, *Why GDPR Is Bad News for the Small Business*, NICHEMARKET (June 9, 2018), https://www.nichemarket.co.za/blog/gdpr-bad-news-small-business/ [https://perma.cc/7DZ5-VMPL].

[17] *See* Albrecht, *supra* note 12, at 287–89.

Although drafters designed the regulation to only protect EU citizens, "the borderless nature" of the internet and e-commerce gives the GDPR a much wider reach.[18] Specifically, since this new regulation applies to any processor of EU-citizen data, the GDPR creates important international implications, as it regulates many large companies operating and headquartered *outside* of the EU territories.[19] "For example, [if] a U.S. airline is selling services to someone out in the UK, although the airline is located in the [United States], they are still required to comply with [the] GDPR because of the European data being involved."[20] In fact, reports estimate that since the GDPR became effective, about half of the U.S. companies regulated by the GDPR likely violated such regulatory requirements.[21] For example, the U.S.-operated company Facebook received particular scrutiny for its privacy dealings after it experienced "improper harvesting of user data by the political profiling firm Cambridge Analytica" in 2018.[22] Already, U.S.-based companies like Facebook, its subsidiaries, WhatsApp and Instagram, and internet powerhouses like Google, face lawsuits for failure to comply with the GDPR.[23]

The GDPR "ha[s] roots in U.S. privacy law and policy," as the United States grappled for years with similar regulatory issues in relation to its many large, innovative technology companies.[24] As such, not only does the GDPR affect U.S. businesses, but it also heavily encourages the United States to adopt similar standards.[25] For instance, the state of California has already begun to develop GDPR-like legislation as it recently passed its own digital privacy law, set to take effect in January 2020.[26]

---

[18] Chen, *supra* note 4.

[19] Rossow, *supra* note 3.

[20] *Id.*

[21] *Id.*; *see* PRICEWATERHOUSECOOPERS, PULSE SURVEY: US COMPANIES RAMPING UP GENERAL DATA PROTECTION REGULATION (GDPR) BUDGETS 3 (2017) [hereinafter PWC]; *Corporate GDPR Preparations to Stretch Past May 2018*, PRICEWATERHOUSECOOPERS (2017), https://www.pwc.com/us/en/services/consulting/cybersecurity/general-data-protection-regulation/pulse-survey-insights.html [https://perma.cc/MPS2-M6S5]; *Who Must Comply*, GDPR EU.ORG, https://www.gdpreu.org/the-regulation/who-must-comply/[https://perma.cc/H8HN-JR3P].

[22] Chen, *supra* note 4.

[23] Michael Kaplan, *Facebook and Google Are Already Facing Lawsuits Under New Data Rules*, CNN (May 25, 2018, 4:24 AM), https://money.cnn.com/2018/05/25/technology/gdpr-compliance-facebook-google/index.html [https://perma.cc/NW6Z-GXC5].

[24] Julie Brill, Comm'r, Fed. Trade Comm'n, Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation Ghostery/Hogan Lovells Data Privacy Day (Jan. 21, 2016) (transcript cited to as 2016 WL 355519 (2016)).

[25] *Id.*; *see generally* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.100–199 (demonstrating how U.S. states have begun drafting GDPR-like legislation).

[26] Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/6PFV-RQKR].

Ultimately, the burdens of heightened data privacy requirements were quickly revealed in the form of new fines, increased litigation, and the need for internal reorganization.[27] Consumers, however, do not seem to appreciate these increased protections, as they rarely read the updated privacy terms and conditions provided via notifications and email notices.[28] Such behavior suggests that consumers would prefer to keep receiving curated and personalized services, like "New Music Friday" Spotify playlists,[29] rather than gaining transparency over how those services are so thoughtfully created.[30]

This note argues that the benefits of the GDPR's increased data privacy are overshadowed by the burdens GDPR imposes on businesses. As the United States moves towards adopting similar data privacy legislation,[31] Congress should create laws with simpler restrictions, clearer guidelines, and more lenient standards, so the consumer benefits of data privacy reform can be achieved without imposing such large burdens on companies.[32]

Rather than parsing through ninety-nine articles and over two hundred pages of complex regulatory text,[33] this argument is supported primarily through case studies of major international tech companies focusing on how they collect and utilize user data, how the GDPR impacted them thus far, and how their practices and products have changed and will continue to evolve moving forward. To identify the shortcomings of the GDPR and weigh its benefits, Part I of this note details the general policy foundations backing the GDPR and identifies some of the issues and concerns that the GDPR aims to address. Part II analyzes how tech companies use personal data and why such data collection is so valuable. Part III then balances how the GDPR may benefit

---

[27] *See* Kaplan, *supra* note 23.

[28] *See* Chen, *supra* 4.

[29] *See New Music Friday*, SPOTIFY, https://open.spotify.com/playlist/37i9dQZF1DX4JAvHpjipBk [https://perma.cc/L8QU-KQ2H].

[30] *See* Daniel Terdiman, *Spotify Exec: We Collect an 'Enormous Amount of Data on What People Are Listening to, Where, and in What Context,'* VENTUREBEAT (Feb. 24, 2015 1:27 PM), https://venturebeat.com/2015/02/24/spotify-exec-we-collect-an-enormous-amount-of-data-on-what-people-are-listening-to-where-and-in-what-context/ [https://perma.cc/28VU-QSZ8].

[31] *See* Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'l ASS'N. PRIVACY PROFESSIONALS (July 31, 2019), https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/YR84-W7C2].

[32] *See generally* Chen, *supra* note 4 (discussing the heavy burdens the GDPR imposes on companies and how the current benefits of the GDPR are costly and inefficient, as most consumers do not read the privacy updates sent to them).

[33] *See* Parliament and Council Regulation 2016/679 of April 27, 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), 2016 O.J. (L 119) 1[hereinafter GDPR]; Rossow, *supra* note 3; Tripwire Guest Authors, *supra* note 9.

consumers while also harming businesses that provide services via the internet. Because this issue is constantly and rapidly developing on a global scale, Part IV considers how the GDPR has already begun to change privacy laws in the United States. Accordingly, Part V identifies which of the essential GDPR clauses effectively protect user data, compared to those clauses that damage businesses and consumers alike. Part V closes with suggestions for how innovative state legislatures, and more importantly Congress, might achieve a better balance in their development of privacy laws by adopting common legislative resolutions such as grace periods and private letter rulings.

I. THE EVOLUTION OF DATA PRIVACY LAW IN THE EUROPEAN UNION

Since its conception, consumers, policy makers, and even some businesses have supported and positively received the GDPR.[34] Such support is a natural extension of the increasing fear of tech companies violating consumer privacy and the rising demand that individual personal data should remain private.[35] The roots of this fundamental notion that individual autonomy ought to be prioritized can be traced to elements of early U.S. privacy doctrine but have also developed in international contexts.

A. European Union Regulatory History

Formalized data privacy regulation in the EU began in the 1950s, when the Council of Europe adopted the European Convention on Human Rights and formed the European Court of Human Rights to enforce privacy regulations on each of the EU member states.[36] Amongst other goals, the Convention focused on the protection of privacy and the right to private life.[37] It was not until 1981, however, that the Council of Europe developed the first legally binding regulation on data protection, the Data Protection Convention.[38] Soon after, in 1990, the EU stepped in to adopt such regulation, with the goal of harmonizing privacy laws

---

[34] *See, e.g.*, Dennis Dayman, *Stop Whining, GDPR Is Actually Good for Your Business*, NEXT WEB (Apr. 2018), https://thenextweb.com/contributors/2018/03/18/stop-whining-gdpr-actually-good-business/ [https://perma.cc/GC6F-2L26]; Hern, *supra* note 7.

[35] Sapna Maheshwari, *Hey, Alexa, What Can You Hear? And What Will You Do with It?*, N.Y. TIMES (Mar. 31, 2018), https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html/ [https://perma.cc/ZYF5-AC6Q].

[36] Stefan Kulk & Frederik Zuiderveen Borgesius, *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 301, 302 (Jules Polonetsky et al. eds., 2018).

[37] *Id.*

[38] *Id.* at 308.

throughout the member states.[39] The EU finally adopted the DPD[40] after five years of revisions and debate.[41]

The DPD's primary purposes included "protect[ing] the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" and "safeguard[ing] the free flow of personal data between EU member states."[42] Unlike regulations, directives such as the DPD do not mandate compliance, but rather serve as a goal from which individual EU member states may model and implement their unique laws.[43] The flexibility of the directive meant that once the EU adopted the DPD, the twenty-eight member states of the EU had full discretion over how they chose to develop their own, individual data privacy laws for their country.[44]

B. The Right to an Explanation and the Right to Be Forgotten

Two of the most essential notions developed in the DPD, which the EU more explicitly adopted in the GDPR, include the "right to an explanation" and the "right to be forgotten."[45] The right to explanation is straightforward: it is "a right to information about individual decisions made by algorithms."[46] This theory implies that companies ought to create algorithms and make data collection practices transparent enough such that individuals can understand what data companies collect, how companies use this data, and what company decisions follow as a result.[47]

Meanwhile, a more complex theory known as the right to be forgotten demonstrates how a theory on privacy can become highly complicated when embedded in legislation. The right to be forgotten, which is also referred to as the "right of erasure," or the "right to deletion," asserts that an individual should maintain the right to request for a company to remove information about that individual from the internet.[48] Originally called "subject access rights," the

---

[39] *Id.*

[40] *Id.* The DPD was formerly known as 95/46/EC of the European Parliament and of the Council of 24 October 1995. *Id.*

[41] *Id.*

[42] *Id.*

[43] Petersen, *supra* note 10, at 12.

[44] *Id.*

[45] Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for*, 16 DUKE L. & TECH. REV. 18, 20, 68 n.194 (2018).

[46] Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 189 (2019).

[47] *Id.* at 213–14.

[48] BRYAN CAVE LEIGHTON PAISNER LLP, CALIFORNIA CONSUMER PRIVACY ACT (CCPA) PRACTICAL GUIDE 8 (2018); *see* Rossow, *supra* note 3.

DPD formalized the right to be forgotten in Article 12, which included the right to "rectify, erase or block [one's personal] data."[49]

As one of the few data privacy and algorithmic harm cases to make it to the highest EU court, the Court of Justice of the European Union (CJEU),[50] *Google Spain SL v. Agencia Española de Prot. de Datos*[51] serves as a particularly interesting application of privacy law principles. In *Google Spain SL*, the CJEU held that at a consumer's request, "search engines must remove links to material that 'appear[s] to be inadequate, irrelevant or no longer relevant, or excessive . . . in light of the time that has elapsed,'" as a right for such individual's privacy.[52] However, the court failed to indicate whether the decision would apply to companies other than search engines or if such obligations extended beyond the EU, deciding that courts need to determine each issue on a case-by-case basis.[53] As such, while the GDPR promotes similar theories and values as *Google Spain SL*, it also presents similar questions such as how, and against whom, will the EU practically enforce the right to be forgotten.[54]

C. Adoption of the GDPR

With over twenty years since the adoption of the DPD, the EU realized it needed to adapt its legislation to the digital age and address issues such as the rise of digital marketing and data storage.[55] The EU took around three years to draft and develop the GDPR, which became effective as of May 25, 2018.[56] In addition to updating the DPD, the EU aimed to create a more unified code for the EU member states to follow.[57] Because legislators drafted the GDPR as a regulation rather than a directive, the GDPR serves as

---

[49] Edwards & Veale, *supra* note 45, at 38 ("Although the US lacked an omnibus notion of data protection laws, similar rights emerged in relation to credit scoring in the Fair Credit Reporting Act 1970.").

[50] Brill, *supra* note 24.

[51] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014.).

[52] Brill, *supra* note 24 (quoting *Google Spain SL*, Case C-131/12, ¶ 93).

[53] *Id.* One interesting pushback on the right to be forgotten theory is that it must be balanced against rights to freedom of speech and the right for people to have information. *See* Rossow, *supra* note 3.

[54] The CJEU recently found that the right to be forgotten can only be applied in the EU, considering, amongst other factors, how the right to be forgotten may conflict with the First Amendment in the United States. This decision further highlights the complicated theories required to support and enforce the GDPR internationally. *See* Ben Kochman, *Google Must Only Apply 'Right to be Forgotten' in EU*, LAW360 (Sept. 24, 2019), https://www.law360.com/articles/1202254/print?section=cybersecurity-privacy [https://perma.cc/4JXN-V9WE].

[55] *See* Kohler, *supra* note 16; Rossow, *supra* note 3.

[56] Hern, *supra* note 7.

[57] Rossow, *supra* note 3.

a binding standard with which all EU member states must comply, instead of adopting their own individual legislation as they did under the governance of the DPD.[58]

In addition to creating an expansive reach for the GDPR, the drafters of the regulation created an incredibly lengthy and more developed legislation compared to the DPD, as the GDPR includes a total of ninety-nine complex, dynamic, and often vague articles.[59] For example, one of the clearer provisions, Article 3, details that companies, whether founded and headquartered in the EU or not,[60] are subject to GDPR if:

> (1) The business has a presence in an EU country; (2) Even if there is no presence in the EU, the company still processes personal data of European residents; (3) There is more than [two hundred fifty] employees; and (4) Even if there is fewer than [two hundred fifty] employees, if the data-processing impacts the rights and freedoms of its data subjects.[61]

By having such broad-reaching legislation, the regulation intentionally gives expansive rights to individuals and greatly impacts businesses. Amongst other initiatives, the GDPR aims to give users more control over how companies handle the users' personal data and what data collection such companies must reveal, delete, or hold.[62] This new standard aims to enable regulators to seamlessly enforce guidelines across EU jurisdictions rather than in each individual member state, while also encouraging strict enforcement measures.[63] Such regulatory goals are clearly reflective of the right to explanation and the right to be forgotten, which developed in earlier privacy regulations.[64] For example, Article 9(2) states that, "[e]very act of processing personal data in the GDPR requires a lawful ground of processing."[65] Further, Article 22 requires that, "'suitable measures to safeguard the data subject's rights' must be put in place, which should include 'at least the right

---

[58] *Id.*

[59] *Id.*; *see* GDPR, *supra* note 33.

[60] Patrick Hromisin, *U.K.'s First GDPR Enforcement Action Against Non-E.U. Company Marks a Significant Milestone*, SAUL EWING ARNSTEIN & LEHR LLP (Sept. 26, 2018), https://www.saul.com/sites/default/files/Cybersecurity_092518.pdf [https://perma.cc/P6CX-4SVS] ("Article 3(2)(a) of the GDPR states that it 'applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to . . . the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union.'" (quoting GDPR, *supra* note 33, at art. 3(2)(a))).

[61] Rossow, *supra* note 3; *see* GDPR, *supra* note 33, at art. 3; *Who Must Comply*, *supra* note 21.

[62] Hern, *supra* note 7.

[63] *Id.*

[64] *See* Edwards & Veale, *supra* note 45, at 40, 42, 81.

[65] *Id.* at 49 n.129.

to obtain human intervention."'[66] In other words, these articles reflect the right to explanation as they require that companies process data using algorithms created such that companies can decode and explain these algorithms to the data subjects. Similarly, Article 17 states that the "data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay."[67] This regulation solidifies a right to be forgotten by demanding that individual citizens of the EU maintain a right to request that their personal information be erased and no longer processed by data collectors or purchasers of such data.[68]

With such an all-encompassing regulation also comes severe enforcement measures, which the EU Information Commissioner's Office will oversee.[69] As soon as the GDPR went into effect in May 2018, a company's breach of any provision could be punishable by any data protection authority[70] with penalties "up to 4 percent of a company's annual global revenue, or €20 million (about $23 million), whichever is higher."[71] With such a heavy burden of enforcement and a much higher bar for compliance than previously required, the GDPR introduces a "very high standard to meet, requiring that companies invest large sums of money to ensure they are in compliance."[72] Again, although the GDPR only applies to the collection of personal data of EU citizens, because of the global nature of the internet, regulations and corresponding penalties may be enforced against companies internationally—an essential feature of the regulation.[73]

II. HOW COMPANIES USE PERSONAL DATA

Regardless of the evident protection that the GDPR provides to consumers, few consider what the GDPR is protecting consumers *against*. A closer look at current tech company practices demonstrates how companies that process

---

[66] *Id.* (quoting GDPR, *supra* note 33, at art. 22(3)).

[67] GDPR, *supra* note 33, at art. 17(1).

[68] Lindsay Rowntree, *An American Perspective: The Three Worst Things About the EU GDPR*, EXCHANGEWIRE (July 7, 2016), https://www.exchangewire.com/blog/2016/07/07/an-american-perspective-the-three-worst-things-about-the-eu-gdpr/ [https://perma.cc/ABF6-TJZR].

[69] Brian Fung, *Why You're Getting Flooded with Privacy Notifications in Your Email*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/25/why-youre-getting-flooded-with-privacy-notifications-in-your-email/?utm_term=.57e96b8327ef [https://perma.cc/H9D4-JVJZ].

[70] *See* Albrecht, *supra* note 12, at 287–89; Hern, *supra* note 7.

[71] Fung, *supra* note 69.

[72] Rossow, *supra* note 3.

[73] Russell Brandom, *Everything You Need to Know About GDPR*, VERGE (May 25, 2018), https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-require ments-privacy-notice [https://perma.cc/LW99-BFYD].

large amounts of data, such as Google, Amazon, and Spotify, often harmlessly and thoughtfully utilize such information to develop and improve the services that consumers love.[74]

By analyzing how companies utilize the data they collect, it becomes apparent why these companies greatly value the collection of personal information—because such data collection benefits consumers. The GDPR and its supporters tend to portray companies like Facebook as technology giants who prey and profit on the personal information of individuals.[75] To that end, it is true that data processing platforms collect the personal information of users and sell this valuable data to advertising and marketing companies.[76] However, the creation of a strong revenue stream through the sale of data and advertisement metrics enables companies like Facebook to offer their platform to users free of charge.[77] Therefore, given the more stringent requirements of the GDPR, obviously platforms like Facebook, which rely on advertising revenue to operate, want to gain informed consent from as many users as possible so that they may continue to provide their services for free.[78]

Furthermore, the cynical portrayal of data processors fails to consider that most companies collect data to enhance the consumer experience.[79] It has been revealed that as a young company, Facebook previously worked within the bounds of U.S. federal limitations to exploit user data to create strategic partnerships with other data companies as leverage to grow the power of its platform.[80] Skeptics may perceive such behind-the-scenes, third-party partnerships as shady and exploitive of individual consumers.[81] In reality, big technology companies such as Amazon, Google, Facebook, and Spotify use most gathered, tracked, and shared data to improve and integrate their platforms, develop new and better products, expand customer support, and find new revenue channels.[82] For example, when

---

[74] *See, e.g.*, Glen Sears, *GDPR Data Exports Reveal Spotify Tracks Absolutely Everything About You*, DANCE MUSIC NORTHWEST (Aug. 3, 2018), http://dancemusicnw.com/spotify-gdpr-data-exports-user-tracking/ [https://perma.cc/H3AL-WJG7].

[75] *See* Chen, *supra* note 4.

[76] *See* Youyou Zhou, *An Oregon Family's Encounter with Amazon Alexa Exposes the Privacy Problem of Smart Home Devices*, QUARTZ (May 25, 2018), https://qz.com/1288743/amazon-alexa-echo-spying-on-users-raises-a-data-privacy-problem/ [https://perma.cc/9AB8-4XVQ].

[77] Kohler, *supra* note 16.

[78] *See* Chen, *supra* note 4; Kohler, *supra* note 16.

[79] Sears, *supra* note 74.

[80] Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html [https://perma.cc/M5NM-URHF].

[81] *See id.*

[82] *See id.*; Sears, *supra* note 74.

explaining how Amazon collects data from its Alexa smart home devices, Amazon claims it uses actual recordings to help fulfill customer requests and improve their own services, and only shares general personal details like ZIP codes with third parties—not actual customer recordings or specific personal information.[83] Accordingly, Amazon expressed worry that the requirement for users to opt-in to data collection may slow popular features and weaken other aspects of the Amazon user experience that customers enjoy (e.g., Amazon's product recommendations, which are suggested based on the customer's browsing history on the platform).[84] Advertising representatives from Spotify echoed that they approach data collection as a tool to provide more curated playlists as well as personalized ads to customers, to provide an optimized, more affordable customer experience while also maximizing Spotify's own revenue.[85]

To create such a personalized experience, many advanced companies utilize machine learning algorithms to process and predict data outcomes on their own, without human input, to maximize use of employee time and also expedite the efficiency of products and services.[86] Humans have an incredibly difficult time attempting to breakdown and interpret such complex algorithms, especially in the manner that the GDPR requires.[87] For context, LinkedIn collects over one hundred thousand variables for each user that their programs feed into the machine learning models.[88] As a result, to respond to the incredibly complex demands of the GDPR, companies like Amazon say that the GDPR "require[s them] to divert significant resources to administrative and record-keeping tasks and away from invention on behalf of customers."[89]

---

[83] Maheshwari, *supra* note 35.

[84] Ben Kochman, *Tech Giants Want Uniform Privacy Law but No GDPR*, LAW360 (Sept. 26, 2018), https://www.law360.com/articles/1086064/tech-giants-want-uniform-privacy-law-but-no-gdpr [https://perma.cc/7TAA-AMCN].

[85] Terdiman, *supra* note 30.

[86] Edwards & Veale, *supra* note 45, at 26.

[87] *See id.* at 26, 59 (explaining how the more developed, advanced, and effective a machine learning system is, the more difficult it will be for a human to reverse-engineer and decode).

[88] *Id.* at 59.

[89] Kochman, *supra* note 84 (quoting Andrew DeVore, Vice President and Associate General Counsel of Amazon).

III. THE EFFECTS OF THE GDPR

A. Successes of the GDPR

The GDPR undeniably stands at the forefront of privacy and data protection for consumers.[90] Given the context of data privacy theories and the legislative history of the DPD, the GDPR was generally received with high praise.[91] Undoubtedly, the GDPR provides more autonomy and protection for individual citizens, particularly at a time when companies value and exploit personal data more than ever.[92] Because of the GDPR, consumers have the ability to control who they share their data with and to maintain more meaningful consent during such process.[93] The GDPR achieves such protection by enabling individuals to see what personal information companies are collecting, and allowing individuals to transfer such data between networks if they do not consent[94] to the data provisions and privacy policies provided by each company.[95]

Furthermore, this heightened protection for individuals creates a higher standard for businesses, as the law requires that they provide easy consumer access to personal data and that companies notify the public of a data breach within seventy-two hours of such discovery.[96] Such regulation may also lead corporations to take extra precautionary measures such as hiring a data protection officer and revising their policies.[97] Moreover, the higher standards set for corporations now give individuals the ability to hold companies accountable "by withholding consent for certain uses of data, requesting access to their personal information from data brokers, or deleting their information from sites altogether."[98] As a result, the GDPR requires that companies provide greater transparency, reliability, and accountability to their customers by developing more consumer-friendly and trustworthy policies and procedures.[99] For example, Facebook's Chief Privacy Officer, Erin Egan, said that Facebook made their "policies clearer,

---

[90] *See* Albrecht, *supra* note 12.

[91] *See* Rossow, *supra* note 3.

[92] *See* Tripwire Guest Authors, *supra* note 9.

[93] Chen, *supra* note 4.

[94] *See* Intersoft Consulting, *GDPR Consent*; GDPR-INFO.EU, https://gdpr-info.eu/issues/consent/ [https://perma.cc/4PMG-N5WB] (discussing the GDPR's various articles and recitals that require that a data subject's consent be "freely given, specific, informed and unambiguous").

[95] Brandom, *supra* note 73.

[96] Fung, *supra* note 69.

[97] *Id.*

[98] Hern, *supra* note 7.

[99] *See* Albrecht, *supra* note 12, at 288–89; Kaplan, *supra* note 23.

[their] privacy settings easier to find[,] and introduced better tools for people to access, download, and delete their information."[100]

Additionally, commentators celebrate the GDPR on a legislative front, as it provides more consistency and uniform enforceability to regulations than the DPD or any other data privacy law to date.[101] As mentioned above, legislators drafted the GDPR as a regulation, meaning it requires compliance of all member states, therefore forcing the member states to replace their various, individually existing provisions.[102] Giving the EU its first unified privacy regulation, the GDPR sets one, harmonious standard for all member states to implement.[103] These heightened standards create positive results, as each of the twenty-eight member states will now be held to the same, cohesive standards and the Information Commissioners Office may enforce the GDPR consistently throughout the EU.[104]

The last, and perhaps most important reason the GDPR causes such substantial impact, is because of the heavy fines that it threatens against those in violation of the regulation.[105] These fines make the GDPR carry true weight and force companies to take action to comply with the regulation to effect real change.[106] As such, not only does the GDPR require companies to update their existing platforms, but it also requires companies to deeply consider privacy protection issues from the conception of all new products.[107]

B. How the GDPR Hurts Companies

While the GDPR provides apparent benefits to consumers,[108] the overall effect of this regulation on global companies has been negative. Given how companies utilize personal data collection, it is clear that data and privacy regulation stymies the success and development of businesses that rely on the collection of data.[109] In addition to imposing stringent regulations on data collection, the GDPR drafters made certain errors in its drafting, such as enforcing unclear and overly demanding provisions, which go beyond

---

100 Kaplan, *supra* note 23.

101 *See* BRYAN CAVE LEIGHTON PAISNER LLP, *supra* note 48, at 2, 5.

102 Albrecht, *supra* note 12, at 289.

103 *Id.*

104 *Id.*

105 *Id.* at 287.

106 *See* Stan Horaczek, *Here's Why You've Been Getting So Many Privacy Policy and Terms of Service Updates Lately*, POPULAR SCI. (Apr. 26, 2018), https://www.popsci.com/gdpr-privacy-policy-update-notices [https://perma.cc/2PR8-KSN8].

107 *Id.*; *see* Petersen, *supra* note 10, at 15.

108 *See supra* Section III.A.

109 *See supra* Part II.

protecting privacy and directly harm data processing platforms.[110] Such errors and stringent regulations make the GDPR as a whole unclear and unduly burdensome.[111]

1. Unclear Provisions Frustrate Compliance and Are Unduly Burdensome

Certain provisions of the GDPR, such as the "legitimate interest" exception, exemplify how the GDPR is complex, obtuse, and difficult to interpret. This provision states that if a data processor demonstrates a necessary and legitimate interest in collecting personal data, they do not need to gain consent from the user.[112] For instance, if a pizzeria servicing EU citizens offers a delivery service for their food products, they would possess a legitimate interest in collecting a customer's address and basic contact information.[113] In this scenario, the pizzeria requires such information as a necessity to fulfill their delivery service, and the customer could reasonably expect that the pizzeria would need to collect such personal information for the sole purpose of providing the delivery.[114] Accordingly, under the GDPR, the pizzeria would be exempt from obtaining explicit consent from the customer via an opt-in portal before processing such data.[115]

Although seemingly simple, the vague "legitimate interest" provision does not provide sufficiently detailed instructions to guide companies on whether or not their interests qualify as legitimate, potentially leading companies to resort to a number of incorrect resources and unnecessary concerns.[116] For example, companies commonly worry that they may be liable for data collected by a third-party partner with whom they share a business relationship.[117] In other words, even if a company determines that they qualify for a legitimate interest exception, it is unclear if this exception would apply to any transaction they conduct with another party.[118]

---

[110] *See, e.g.*, *Legitimate Interest*, GDPR EU.org, https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/ [https://perma.cc/U2KM-US3V] (explaining unnecessarily complex provisions of the GDPR).

[111] *See* Matt Novak, *Dozens of American News Sites Blocked in Europe as GDPR Goes into Effect Today*, GIZMODO (May 25, 2018), https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542 [https://perma.cc/4MCF-DMLJ] (discussing companies who chose to cease service to E.U. citizens due to the uncertainties of the GDPR).

[112] *See Legitimate Interest*, *supra* note 110; GDPR, *supra* note 33, at art. 6.

[113] *Legitimate Interest*, *supra* note 110.

[114] *Id.*

[115] *Id.*

[116] *See id.*

[117] Brandom, *supra* note 73.

[118] *See id.*

Moreover, many companies who may not be governed by the GDPR often misinterpret GDPR provisions and make precautionary changes as a result.[119] Such misguided attempts towards compliance may include unnecessary updates of terms and conditions or sending customers unnecessary email updates of policy changes.[120] As a result of unclear drafting and company confusion, such practices may backfire if consumers decide to unsubscribe from services due to the consumers' emails flooding with superfluous updates.[121] Ultimately, while companies may not need to comply with the GDPR, for example those which qualify for the legitimate interest exception, a simple misunderstanding of the GDPR's confusing legislation may cause companies to take unnecessary actions that discourage and deter their clients.

The GDPR's standards are unduly burdensome as evidenced by the difficulty in complying with their terms due to their lack of clarity. Without regard for the complex process of understanding the GDPR, the regulation still imposes very strict repercussions for noncompliance.[122] The GDPR grants no grace periods for noncompliance, and does not provide any grandfather provisions or appeal procedures for companies deemed to be noncompliant.[123] For instance, various claimants filed complaints for noncompliance against Facebook, Google, WhatsApp, and Instagram, with international data regulators in several countries across the EU "as soon as the law went into effect at midnight."[124] Moreover, the enforcement officials of the EU, the Article 29 Working Party, maintain "the exclusive and unchallengeable right to search and seize [any] records in question," regardless of the size or location of the company.[125] As a result, one study revealed that nearly 70 percent of businesses failed to address data requests from individuals within the one-month span required by the GDPR.[126] Another study claims that before the enactment of the GDPR, over half of international businesses surveyed feared that they would face fines due to the passing of the regulation.[127] Without an

---

[119] Lydia Belanger, *Here's Why Your Inbox Is Filled with Privacy Policy Emails*, ENTREPRENEUR (May 29, 2018), https://www.entrepreneur.com/article/314170 [https://perma.cc/XD3R-KD3T]; *see* Hern, *supra* note 7 ("The world's largest companies have updated their sites to comply with [the] GDPR.").

[120] Belanger, *supra* note 119.

[121] *Id.*

[122] Brill, *supra* note 24.

[123] Rowntree, *supra* note 68.

[124] Kaplan, *supra* note 23.

[125] Rowntree, *supra* note 68.

[126] Press Release, GlobeNewswire, The Majority of Businesses Are Failing to Comply with GDPR (Sept. 13, 2018).

[127] OVUM, DATA PRIVACY LAWS: CUTTING THE RED TAPE, at 7 (2018), https://www.intralinks.com/resources/analyst-reports/ovum-report-data-privacy-laws-

opportunity for grace periods or appeals, complying with the GDPR's complicated provisions is not only a highly unpredictable endeavor, but the regulation also fails to encourage and teach companies how to become compliant moving forward.[128]

2. Compliance is Unreasonably Costly

Given such unclear provisions and strictly enforced regulations, all data processors operating internationally now hold the responsibility to invest in their own due diligence to determine if they must comply with the GDPR legislation.[129] According to a PricewaterhouseCoopers survey conducted in December 2016, 68 percent of U.S.-based companies already expected to spend between $1 million and $10 million to comply with the GDPR requirements.[130] Additionally, a global study that examined several different industries found that two-thirds of companies surveyed expected the GDPR to force the businesses to change their strategies, while 52 percent still feared that their businesses would be fined.[131]

The extensive investments that companies must allocate toward a multitude of precautionary measures yield striking statistics on how the GDPR negatively impacts businesses.[132] First, companies that even remotely operate in the EU may heavily consider retaining outside counsel or entirely hiring individuals to determine if the GDPR even applies to the company at all.[133] Once a company determines that it needs to be GDPR compliant, it must take a number of additional steps. To ensure basic GDPR compliance, companies should develop a data breach response plan, hire a data protection officer or team, and record and document all compliance measures.[134] Assuming companies even have the capacity to take on such compliance requirements, they will likely need to take extra precautionary measures such as hiring full-time data protection personnel, significantly investing in technology updates and solutions, and having funds prepared and allocated

---

cutting-red-tape?utm_source=blog&utm_medium=blog&utm_campaign=146168+2015-12+global-corporate-knowledge-q4+dsov+campaign&utm_content=december2015 [https://perma.cc/39ZS-FF3P].

128 Rowntree, *supra* note 68.

129 *See id.*; Tripwire Guest Authors, *supra* note 9.

130 PWC, *supra* note 21, at 2.

131 OVUM, *supra* note 127, at 1.

132 *See* Rossow, *supra* note 3.

133 *See generally* BRYAN CAVE LEIGHTON PAISNER LLP, *supra* note 48 (suggesting the many ways in which retaining a law firm may be beneficial for navigating the GDPR).

134 Rossow, *supra* note 3.

toward litigating claims and possibly pay fines.[135] Such implications essentially create a fine in itself for simply servicing EU citizens.

Throughout the compliance process, companies will also likely incur additional expenses when choosing whether or not to maintain their regular business practices.[136] For example, on one hand, the GDPR will require many large companies to perform additional due diligence when assessing their current partnerships and expansions, causing such businesses to move forward with heightened caution in forming new deals with third parties that may expose such companies to greater risk or liability in GDPR compliance.[137] On the other hand, major U.S. news outlets, including the *Los Angeles Times*, determined that such additional risks and costs outweigh the value of their EU business and decided to entirely block their services from EU citizens, at least until those companies gain more clarity and certainty on how to adhere to the new regulations.[138] Just a year after the GDPR passed, a National Bureau of Economic Research study reported that venture capital investment in European startups reduced by over $3 million—leading to an estimated 3,000–30,000 fewer jobs.[139] These emerging practices demonstrate the fear that the unclear and burdensome provisions incite in companies worldwide. Now, companies must merely discern whether they need to comply with the GDPR and take steps to become compliant or decide to close off services to EU data subjects altogether. Regardless of their path, these companies will spend and likely lose money in the process.

Furthermore, requiring compliance with such legal obligations assumes that companies hold the capacity to do so or carry the funds to face the consequences of falling out of compliance, thus setting an even higher barrier to entry for small businesses operating online.[140] Smaller data-processing businesses already struggle to build their technology and

---

[135] *See* Tripwire Guest Authors, *supra* note 9.

[136] *See generally* Joe Castelluccio, *Missiles, Malware and Merger Management: Why Cybersecurity and Data Privacy Matter to M&A Practitioners—Part II*, BLOOMBERG L. (Oct. 10, 2018), https://news.bloomberglaw.com/mergers-and-antitrust/insight-missiles-malware-and-merger-management-why-cybersecurity-and-data-privacy-matter-to-m-a-practitionerspart-ii [https://perma.cc/F3X2-2DTJ] (discussing the multitude of factors companies need to assess in determining how to adapt their regular practices to comply with the GDPR; for example, in double-thinking whether going through a merger will create additional GDPR implications).

[137] *See id.*; Brandom, *supra* note 73.

[138] Novak, *supra* note 111; *see* Rossow, *supra* note 3.

[139] Jian Jia et al., The Short-Run Effects of GDPR on Technology Venture Investment 4 (Nat'l Bureau of Econ. Research, Working Paper No. 25248, 2018).

[140] *See* Jon Markman, *GDPR Is Great News for Google and Facebook, Really*, FORBES (May 22, 2018), https://www.forbes.com/sites/jonmarkman/2018/05/22/gdpr-is-great-news-for-google-and-facebook-really/#7ce4a01548f6 [https://perma.cc/BQ7P-TCKV].

databases, so having to start fresh and comply with the GDPR presents a much greater hurdle to small companies than the GDPR poses for powerhouses like Facebook or Google.[141] For instance, a consumer would probably quickly and mindlessly consent to a privacy pop-up on their Facebook account, which they use regularly and trust as a widely-used platform, than they would consent to a notification from a company of little to no reputation, which they can easily unsubscribe from via email.[142]

The combination of unclear, vague, and lengthy legislation, along with strict enforcement provisions, create the perfect circumstances for a flood of litigation, as all companies and firms struggle to predict which practices and interpretations of the GDPR are correct.[143] In just the first day that the GDPR was enacted, Facebook and Google were "hit with a collective $8.8 billion lawsuit."[144] Similarly, not even four months after the GDPR became effective, the United Kingdom Information Commissioner's Office issued its first extraterritorial enforcement of the GDPR, providing just one example of a claim filed internationally under the regulation.[145] Fundamentally, because the GDPR fails to provide context and instruction, for example, in terms of what a "reasonable" level of protection is, the courts will likely be the only resource to resolve the inevitable barrage of legal disputes to come.[146]

C. Facebook and the GDPR: A Case Study

Facebook is an international social media platform that operates free to users, primarily by selling advertisement space and users' personal information to advertising and marketing companies.[147] The GDPR continues to target Facebook as one of the businesses most commonly affected by the data privacy

---

[141] Kohler, *supra* note 16.

[142] *Id.*

[143] *See* Chen, *supra* note 4; Hern, *supra* note 7.

[144] Rossow, *supra* note 3.

[145] Hromisin, *supra* note 60. The enforcement action required Canadian data processor Aggregate IQ to "[c]ease processing any personal data of U.K. or E.U. citizens obtained from U.K. political organizations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes," or otherwise be subject to GDPR fines. *Id.* (alteration in original); *see also* White and Williams LLP, *Corporate Statements About GDPR Spark Securities Class Action Lawsuit*, JD SUPRA (Sept. 7, 2018), https://www.jdsupra.com/legalnews/corporate-statements-about-gdpr-spark-58240/ [https://perma.cc/S6LV-LYQB] (discussing implications of the GDPR on securities class actions).

[146] *See* Rossow, *supra* note 3.

[147] *See* Greg DePersio, *Why Facebook Is Free to Use (FB)*, INVESTOPEDIA (Dec. 3, 2015), https://www.investopedia.com/articles/markets/120315/why-facebook-free-use.asp [https://perma.cc/FY5W-6DTE]; *What Is Facebook*, GCF GLOBAL, https://edu.gcfglobal.org/en/facebook101/what-is-facebook/1/.

regulation.[148] As such, Facebook's responses and changes throughout the development of the GDPR serve as a particularly interesting example of the impacts that the GDPR imposes on large businesses that gather and utilize the data of EU data subjects.

Most recently, Facebook was the subject of increased scrutiny after the *New York Times*, *The Observer of London*, and *The Guardian*[149] revealed that Cambridge Analytica, a British political data firm, hacked and harvested the personal data of fifty million Facebook users.[150] This scandal, soon followed by the implementation of the GDPR, led Facebook to make a number of substantial changes to its policies and products with the end goal of providing users more autonomy over their privacy and personal information.[151] Amongst other updates, Facebook unified its privacy options and built an "access your information" portal which allows consumers to locate, download, and delete certain personal data from the website.[152] Representatives from Facebook commented that the platform required every user to agree to the new terms of service and encouraged them to opt-in to facial recognition technology as a heightened security precaution.[153] Like many other data processing companies collecting EU information, Facebook enforced such compliance and privacy measures by using in-product notifications, as well as informing users about their new privacy rights through consumer education campaigns.[154] More specifically, the Facebook platform flags European users on the service and informs these select users of Facebook's new terms and conditions, requiring that users either decline the collection of "sensitive data, facial recognition, and use of outside data to inform ads," or that users expressly give "their

---

[148] Rossow, *supra* note 3; *see* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/9BNM-SAQQ].

[149] Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/9BNM-SAQQ].

[150] Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline [https://perma.cc/87MT-N5FL]; Maheshwari, *supra* note 35.

[151] *See* Hern, *supra* note 7.

[152] *Id.*; *see* Kaplan, *supra* note 23.

[153] Hern, *supra* note 7.

[154] *See What Is the General Data Protection Regulation (GDPR)?*, FACEBOOK BUS., https://www.facebook.com/business/gdpr [https://perma.cc/265C-PP4H]; *see also* Hern, *supra* note 7 ("Google took a different tack, quietly updating its products and privacy policies without drawing attention to the changes.").

dedicated attention and consent" to the updated policies in order to continue use of the platform.[155]

To further illuminate the attention and effort Facebook dedicates to GDPR compliance, Facebook representatives publicized that the company spent over eighteen months preparing to ensure compliance.[156] As part of their preparation, Facebook established the largest cross-functional team in the company's history.[157] Consequentially, Facebook's newest privacy protection efforts include an accessible list of privacy principles which explain the company's approach to privacy and data protection, a team dedicated to documenting and ensuring continued compliance efforts, and regular meetings with international regulators, policymakers, privacy experts, and scholars who provide advice and feedback on Facebook's current and future approaches to protecting personal information.[158] It is worth noting that Facebook's efforts to comply with the GDPR were made concurrently with a five-billion-dollar settlement with the United States Federal Trade Commission (FTC)[159] after the Cambridge Analytica scandal.[160]

Despite Facebook's genuine efforts and beliefs that they were in compliance with the GDPR, the company was one of the first corporations targeted with lawsuits upon the passing of the regulation.[161] On the very first day the GDPR became effective, an Austrian non-governmental organization, None of Your Business, filed a series of complaints to the National Data Protection Commission (CNIL), the French data protection authority, seeking €3.9 billion, arguing that, "Facebook [among other tech giants like Google, etc.] is breaking a GDPR rule intended to prevent companies from hoovering up sensitive information like political opinions, religious beliefs, ethnicity and sexuality

---

[155] Nitasha Tiku, *Why Your Inbox Is Crammed Full of Privacy Policies*, WIRED (May 24, 2017), https://www.wired.com/story/how-a-new-era-of-privacy-took-over-your-email-inbox/ [https://perma.cc/JG38-XCHZ].

[156] Chris Foxx, *Google and Facebook Accused of Breaking GDPR Laws*, BBC (May 25, 2018), https://www.bbc.com/news/technology-44252327 [https://perma.cc/2R7Q-J4J3].

[157] *What is the General Data Protection Regulation (GDPR)?*, *supra* note 154.

[158] *Id.*

[159] Under the Federal Trade Commission Act, the FTC is empowered to, among other things, prevent unfair or deceptive acts or practices affecting commerce, seek monetary redress and relief for conduct injurious to consumers, prescribe rules, and make legislative recommendations to Congress. 15 U.S.C. §§ 41–58.

[160] Kelly Makena, *FTC Hits Facebook with $5 Billion Fine and New Privacy Checks*, VERGE (July 24, 2019), https://www.theverge.com/2019/7/24/20707013/ftc-facebook-settlement-data-cambridge-analytica-penalty-privacy-punishment-5-billion [https://perma.cc/3D4F-RKBR].

[161] Rossow, *supra* note 3.

without their users' consent."[162] Moreover, Michael Veale, a technology policy expert at the University College London, speculates that even if consumers demand that Facebook removes their data from the platform, Facebook can still glean personal information about users by tracking their behavior on the platform and other websites.[163]

D. Effectiveness of the GDPR

Despite the consumer-oriented goals of the GDPR, it seems that consumers are either confused by, are indifferent to, or are intentionally ignorant to privacy protections.[164] Overall, privacy regulations may tend to bore and confuse consumers, especially with consumers facing "pop-up fatigue," as they experience an overwhelming influx of privacy notifications and updates as a result of the GDPR.[165] Moreover, even if consumers do care to engage with their new privacy and data protections, a 2008 study showed that it would take the average person roughly 244 hours per year, or about forty minutes per day, to read through all of the privacy policies that applied to them.[166] The study also found that if consumers "did read [the policies] at least once a year, it would . . . cost $365 billion in lost leisure and productivity time,"[167] amounting to a national opportunity cost of $781 billion.[168]

As a result of this large opportunity cost, studies found that consumers rarely read through privacy policies, and that the policies do not promote more rational decision making amongst consumers and generally do not increase transparency in the business to consumer interaction.[169] For example, despite Facebook's multifaceted efforts to protect users and provide GDPR-compliant transparency, the number of daily active European users plummeted by 3 million people, dropping to 279

---

[162] Kaplan, *supra* note 23. Ultimately, Google, who received a similar complaint, had to face a financial penalty of fifty million euros. Comm'n Nationale de l'Informatique et des Libertés [CNIL] [Nat'l Data Prot. Comm'n], Jan. 21, 2019, SAN-2019-001.

[163] Kaplan, *supra* note 23.

[164] *See* Chen, *supra* note 4.

[165] *Id.*; *see* John Constine, *A Flaw-by-flaw Guide to Facebook's New GDPR Privacy Changes*, TECHCRUNCH (Apr. 18, 2018), https://techcrunch.com/2018/04/17/facebook-gdpr-changes/ [https://perma.cc/9QVQ-RE8E].

[166] Horaczek, *supra* note 106 (noting "that was way back in 2008 when people used the internet for an estimated [one] hour, [twelve] minutes per day—a number that has grown to roughly [three] hours, [ten] minutes, [more recently]").

[167] Nate Anderson, *Study: Reading Online Privacy Policies Could Cost $365 Billion a Year*, ARS TECHNICA (Oct. 8, 2008), https://arstechnica.com/tech-policy/2008/10/study-reading-online-privacy-policies-could-cost-365-billion-a-year/ [https://perma.cc/NWJ8-PCB4].

[168] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 INFO. SOC'Y: J.L. & POL'Y 543, 565 (2008).

[169] Anderson, *supra* note 167.

million.[170] Interestingly, users in North America during the same period remained constant.[171] Such statistics suggest that consumers do not truly care about actual privacy standards offered by the platforms they use, but rather that they may be negatively influenced by and turned away from companies with increased privacy disclosures.

Considering the burdens that the GDPR places on companies, coupled with the beneficial but consumer-ignored protections that the GDPR creates, the GDPR threatens significantly negative, lasting impacts on the internet and data privacy processors. One possible outcome of the GDPR is that data processing companies begin to charge or increase their current prices for their services to offset the cost of GDPR compliance and the greater difficulty of generating targeted and relevant marketing.[172] Another potential implication of the GDPR is that if consumers do not consent to a company's data policies, they must delete their account. A final possible result of the regulation is that if a company does not want to invest in understanding and complying with the GDPR, the company can deny service to EU citizens.[173] As a result, the GDPR will likely bring a divide between the EU citizens and the ability to access e-commerce and internet services.[174] Ultimately, between pop-up fatigue, consumers' lack of interest in privacy law, and the potential negative, long-term impacts for both consumers and businesses, the GDPR appears ineffective and not worth the high costs and burdens that the complicated legislation imposes on businesses.[175]

IV. CHAIN REACTIONS: CALIFORNIA'S PROPOSED PRIVACY LAW

Because the GDPR already largely impacts U.S.-based companies, the United States will inevitably begin to update its policies to reflect more GDPR-like privacy law standards. Although the United States historically supported privacy concepts, such as the right to be forgotten,[176] the United States

---

[170] *Facebook Sees Users Decline in Europe amid GDPR and Cambridge Analytica Fallout*, ADAGE (July 25, 2018), https://adage.com/article/digital/facebook-sees-users-flee-europe-gdpr-effect/314384/ [https://perma.cc/HE26-9M7A].

[171] *Id.*

[172] Rowntree, *supra* note 68.

[173] Rossow, *supra* note 3.

[174] *See* Brandom, *supra* note 73.

[175] *See* Chen, *supra* note 4; Tiku, *supra* note 155.

[176] Edwards & Veale, *supra* note 45, at 38 (discussing how the United States featured rights such as the right to be forgotten in relation to credit scoring in the Fair Credit Reporting Act of 1970).

generally maintained a laissez-faire approach to privacy and internet regulation.[177] For instance, in the late 1990s, when the internet began to rapidly evolve, the FTC decided to take a wait-and-see approach to privacy legislation rather than stifling the growth of the internet.[178] However, with the increased attention to data privacy due to the Facebook-Cambridge Analytica scandal and the recent passing of the GDPR,[179] California took a more strict regulatory approach and passed the California Consumer Privacy Act of 2018 (CCPA).[180]

Drafters plan for portions of the CCPA to take effect as early as January 1, 2020.[181] This act serves a similar purpose to the GDPR by establishing a private right of action if a consumer is harmed by a data breach. The act also unifies California privacy law by precluding individuals from using the CCPA as a basis for action under other statutes.[182] Moreover, the CCPA reflects the GDPR as it provides similar policy-oriented protections, such as the right to be forgotten,[183] and similarly enables consumers to demand greater transparency and control over what data companies collect on them and how companies use such data, via requirements like opt-in pop-ups.[184]

Despite the several provisions that serve a similar purpose to the GDPR, the CCPA features notable differences,[185] both for better and for worse. The CCPA is slightly more lenient and clear in defining the penalties for companies who do not comply with the CCPA.[186] Also, the CCPA sets out a number of criteria to help determine what constitutes a "business" that needs to be in compliance.[187] Moreover, if a claimant believes

---

177 *See* McDonald & Cranor, *supra* note 168, at 545.

178 *Id.*

179 *See supra* Section III.C.

180 *See* CAL. CIV. CODE § 1798.150; Hogan Lovells, *California Consumer Privacy Act: The Challenge Ahead – Consumer Litigation and the CCPA: What to Expect*, JD SUPRA (Sept. 28, 2018), https://www.jdsupra.com/legalnews/california-consumer-privacy-act-the-84605/ [https://perma.cc/RCV5-PPKB].

181 Merrit Jones et al., *California Passes Amendments to Consumer Privacy Act*, BRYAN CAVE LEIGHTON PAISNER (Oct. 4, 2018), https://retaillawbclp.com/california-passes-amendments-to-consumer-privacy-act/ [https://perma.cc/MBU4-J36M].

182 Hogan Lovells, *supra* note 180; Wakabayashi, *supra* note 26.

183 *See* Womble Bond Dickinson, *California's New Privacy Act: Update on Amendments*, JD SUPRA (Sept. 7, 2018), https://www.jdsupra.com/legalnews/california-s-new-privacy-act-update-on-63370/ [https://perma.cc/LH73-RZRX].

184 Wakabayashi, *supra* note 26.

185 *See* Bret Cohen et al., *California Consumer Privacy Act: The Challenge Ahead – A Comparison of 10 Key Aspects of the GDPR and the CCPA*, JD SUPRA (Oct. 3, 2018), https://www.jdsupra.com/legalnews/california-consumer-privacy-act-the-73267/ [https://perma.cc/WY8N-VRTE].

186 For example, unlike the GDPR, the CCPA permits a thirty-day cure period for businesses allegedly violating the law before a claim is assessed. *Id.*

187 *Id.*

that a business does not comply with the CCPA, the consumer must file a notice to the business and provide the business with a thirty-day grace period to cure the issue before filing a suit.[188] Additionally, if the company is ultimately found to be non-compliant, the CCPA provides clearer guidelines than the GDPR in explaining what elements will be considered in determining penalties, such as the "nature and seriousness of the misconduct" and "the length of time over which the misconduct occurred."[189] Such penalties are generally less severe on businesses than those of the GDPR, as an attorney general can grant injunctions, but cannot fine companies for more than $2,500 per violation or $7,500 per intentional violation; however, unlike the GDPR, the CCPA does not include a cap on the total number of violations and fines that can be found.[190]

Even if businesses can more easily interpret the standards of the CCPA, which is slightly more forgiving that the GDPR, the CCPA includes a number of differences from the GDPR that will continue to negatively impact businesses. For example, unlike the GDPR, the CCPA does not feature certain standards, such as the requirement that companies notify their customers if the company experiences a data breach.[191] Meanwhile, the CCPA adds additional provisions, such as the requirement that companies include a "[d]o not sell my personal information link on [their] websites and privacy notices."[192] Furthermore, the CCPA applies extraterritorially and applies to companies that do business within California; however, unlike the GDPR, the CCPA includes a carve-out exception for small businesses and non-profit organizations.[193] Overall, the different requirements set by the CCPA add to the difficulties imposed on businesses by the GDPR, due to additional legislative inconsistencies, a greater lack of clarity, and different compliance requirements to meet worldwide.

At a closer look, the dangerous inconsistencies threatened by the CCPA come as no surprise, as legislative history behind the CCPA reveals that drafters rushed writing the bill so that it could be voted on in time.[194] As such, many critics speculate that legislators will need to pass "cleanup bills" to make the legislation less ambiguous and more consistent with the GDPR before the

---

188 *Id.*; CAL. CIV. CODE § 1798.150(b).

189 CAL. CIV. CODE § 1798.150(a)(1)–(2).

190 Cohen et al., *supra* note 185; *see* Jones et al., *supra* note 181.

191 BRYAN CAVE LEIGHTON PAISNER LLP, *supra* note 48, at 2–3 (noting that California already had an existing data breach notification requirement).

192 *Id.* at 5 (internal quotation marks omitted).

193 *Id.* at 3.

194 *Id.* at 1.

legislation goes into effect on January 1, 2020.[195] For example, some proposed amendments already delayed the enforcement of certain provisions of the CCPA to take effect on July 1, 2020, or six months after the new regulation amendments are passed, whichever date comes sooner.[196] During this time, privacy advocates fear that business and technology lobbyists will make an effort to "water . . . down"[197] the legislation, especially considering powerhouses like Google, Facebook, and Verizon each contributed $200,000 to a committee that opposed the proposed CCPA when the legislation was merely a ballot measure.[198] More importantly, several other states continue to introduce their own variations of the GDPR and CCPA, adding to the complex, confusing, and inconsistent landscape of data privacy compliance.[199] Ultimately, given the apparent mistakes caused by rushed drafting of the CCPA, and the economic pressure from technology companies to redraft legislation, the spotlight now shines on Congress to develop a uniform data privacy regulation to truly meet the standards set by the GDPR.[200]

V. PRACTICAL SOLUTIONS FOR U.S. PRIVACY LAW TO AVOID MISTAKES OF THE GDPR

Regardless of whether or not the GDPR effectively achieves its purpose, businesses, data processors, policy makers, and consumers alike increasingly face issues over data privacy.[201] Moreover, because the GDPR is so new and is unlikely to be reformed any time soon, data processors now have to scramble to determine how to adapt to GDPR standards. As Hawaiian senator Brian Schatz proclaimed, data privacy policy is developing rapidly, so effective changes and suggestions must come from an

---

[195] Wakabayashi, *supra* note 26; *see* BRYAN CAVE LEIGHTON PAISNER LLP, *supra* note 48, at 1; Jones et al., *supra* note 181.

[196] Jones et al., *supra* note 181.

[197] Wakabayashi, *supra* note 26.

[198] *Id.*

[199] To date, there are three states with newly signed data privacy legislation, two states with a data privacy bill in a cross-committee stage, ten states with proposed legislation in committees, and four states with tasks forces either substituted for a comprehensive bill or with bills postponed indefinitely. Each of these new legislations vary widely in depth of drafting and data privacy requirements. *See* Noordyke, *supra* note 31; *see also* Issie Lapowsky, *New York's Privacy Bill Is Even Bolder than California's*, WIRED (June 4, 2019), https://www.wired.com/story/new-york-privacy-act-bolder/ [https://perma.cc/2N2C-JHY2] (discussing how New York's New York Privacy Act (NYPA) proposed in May 2019 is more comprehensive than any other currently proposed state privacy act and how the NYPA significantly departs from the standards set by the CCPA).

[200] *See* Allison Grande, *White House Seeks Input on New Approach to Privacy Rules*, LAW360 (Sept. 25, 2018), https://www.law360.com/articles/1086012 [https://perma.cc/2RQL-2NQU].

[201] *See* Rowntree, *supra* note 68.

equally progressive and forward-thinking place, rather than non-progressive federal law.[202] As such, future GDPR-like legislation (i.e., in the CCPA or future federal legislation) may adopt several practical solutions, such as more reasonable grace periods to become compliant and more clear guidelines for such compliance.

A. Simpler Restrictions for Meaningful Impact

Data privacy legislators need to focus on developing simple and reasonably achievable standards for companies required to be compliant, rather than setting regulations like meaningless user consent that ultimately leads to consent fatigue. Technology giants such as Facebook and Amazon attended several U.S. Senate hearings to contribute to the conversation about federal privacy legislation, but urged Congress to use a lighter approach than the GDPR when drafting new standards.[203] Similarly, the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce recommends taking a more outcome-based approach to privacy, which "emphasizes flexibility, consumer protection, and legal clarity" and "focuses on the outcomes of organizational practices, rather than on dictating what those practices should be" and drowning corporations in unclear legal standards.[204] Instead of attacking tech giants with regulations and threatening fines, the NTIA's approach suggests hearing from stakeholders at various corporations, creating a more unified legislative landscape, and ensuring that the FTC implements the proper enforcement tools to carry out these new regulations.[205] Already, the FTC has encouraged Congress to enact federal legislation which would empower the FTC to monitor collection of user data and enforce privacy legislation.[206] Without federal legislation and support, however, the FTC is already highly concerned about the lack of employees and support they have to handle such matters.[207] By simplifying regulations and focusing on what consumers really care about, such as providing access to more

---

[202] Kochman, *supra* 84.

[203] *Id.*

[204] Grande, *supra* note 200.

[205] *Id.*

[206] Cecilia Kang, *F.T.C. Commissioners Back Privacy Law to Regulate Tech Companies*, N.Y. TIMES (May 8, 2019), https://www.nytimes.com/2019/05/08/business/ftc-hearing-facebook.html?login=email&auth=login-email [https://perma.cc/3GEM-C3E4].

[207] Harper Neidig, *FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security*, HILL (Apr. 3, 2019), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security?utm_campaign=Newsletters&utm_source=sendgrid&utm_medium=email [https://perma.cc/NZ88-Y32F].

transparent data breaches, legislators and data processors can work together to great realistic and impactful goals.

B. Clearer Guidelines for Compliance Requirements

Future privacy regulations can provide clearer provisions in privacy legislation to prevent companies from investing excessive money and time in interpreting complex and lengthy regulations. For example, future regulations can provide supplemental provisions to clarify complex and vague concepts, such as legitimate interest or the right to explanation.[208] More specifically, regulators might consider clarifying what kinds of scenarios and business partnerships would fall within having a legitimate interest and accordingly provide examples to illustrate how regulations may be implemented in various circumstances. Drafters should also consider limiting the right to explanation and transparent data processing only for certain procedures that are of importance to consumers. For example, drafters could avoid legislation that governs *all* data processing procedures, including complex machine learning algorithms, which are highly complex and difficult to breakdown[209] and simply exist to make consumer experiences more curated and efficient.[210]

Regulators might also consider offering private letter rulings to companies who need to determine if they must comply with such regulations. Private letter rulings, which are a common practice in U.S. federal income tax law, are "issued (in letter form) to taxpayers in response to requests for advice about their own specific fact situations. Some of these ultimately are developed into Revenue Rulings, which set forth the official position of the IRS on which all taxpayers are entitled to rely."[211] While this practice may require thorough planning and federal resources, it provides a helpful outlet in the context of unclear regulations on issues such as income taxes and internet and privacy law, especially when these regulations impose such heavy fines for noncompliance. Through private letter rulings, companies may correspond with those enforcing privacy laws to ask questions that clarify legislation and submit proposed actions before making high-risk business decisions.[212] Therefore, these procedures would prevent companies from wasting time and resources determining if a certain action would result in a

---

208 *See, e.g.*, Rossow, *supra* note 3.
209 Edwards & Veale, *supra* note 45, at 59.
210 *See* Terdiman, *supra* note 30.
211 JOSEPH BANKMAN ET AL., FEDERAL INCOME TAXATION 45–46 (17th ed. 2017).
212 *See id.*

regulation violation.[213] As a result, by providing official and reliable clarifications of complex legislation, there would be less international flooding of court cases, court confusion, and inconsistencies in interpretation and enforcement.

C. More Lenient Standards

The CCPA provides more flexibility than the GDPR by providing a grace period of thirty days between submitting a claim to a company and filing a lawsuit;[214] however, this addition still sets a stringent standard. In comparison, the U.S. Securities Exchange Commission offers a variety of reasonable grace periods for erroneous filings to compensate for how incredibly technical and complicated their requirements may be.[215] Especially while data processors operate in the unknown in terms of how the GDPR and like legislation will be interpreted and enforced, legislators could provide more fair standards by offering companies a sensible grace period to cure after they are deemed to be out of compliance. Furthermore, just as the CCPA does not require compliance from certain companies like nonprofits, federal regulations could provide clearer and more reasonable fines and sanctions based on the capacity of the non-compliant data processor. More flexibility in enforcement would allow companies to greatly consider their policies and to make genuine efforts toward compliance, while also affording them time to determine ways to maintain the quality of their curated services without having to shut down or stop service to EU data subjects.

CONCLUSION

The heavy burdens that the GDPR imposes on companies, both to determine if they must comply and later to ensure compliance with the GDPR, are not worth the ultimately marginal benefits that the GDPR provides to consumers. As it stands, the lengthy and unclear provisions of the GDPR provide no lenience to companies, regardless of their size and capacity. This strict standard will likely lead to a flooding of court cases

---

[213] *See Private Letter Ruling (PLR)*, INVESTOPEDIA, https://www.investopedia.com/terms/p/plr.asp [https://perma.cc/EJ94-XENM] ("A [private letter ruling] can . . . help a taxpayer confirm whether or not a potential action will result in a tax violation.").

[214] *See* Cohen et al., *supra* note 185.

[215] Eli Bartov & Yaniv Konchitchki, *How Missing SEC Filing Deadlines Affects a Company's Stock Value*, COLUM. L. SCH. BLUE SKY BLOG. (Nov. 27, 2017), http://clsbluesky.law.columbia.edu/2017/11/27/how-missing-sec-filing-deadlines-affects-a-companys-stock-value/ [https://perma.cc/DYH5-BT5G].

and inconsistent enforcement procedures, only adding to the list of expenses that companies will incur as a result of the GDPR.

Despite the faults of the GDPR, many policy workers worldwide, such as those in the state of California, rush to adapt and develop similar legislation. Although California's CCPA will go into effect in January 2020, CCPA drafters, and more importantly federal legislators, may consider a number of solutions to cure and prevent some of the GDPR's pitfalls. Such solutions include focusing on more meaningful and effective privacy protection provisions, providing clearer guidelines for companies through both drafting and enforcement measures, and allowing for more understanding and supportive responses in the event of noncompliance, especially as companies adapt to such new, demanding regulations. Overall, data and privacy protection must adapt to current technologies, but both consumers and data processors alike benefit when legislators consider the actual needs and priorities of both parties during the drafting stage. Increased privacy protections aside, Alexa knows consumers are going to keep shopping on Amazon anyway.

Katherine M. Wilcox†

† J.D. Candidate, Brooklyn Law School, 2020; B.A. University of Southern California, 2017. Thank you to the entire *Brooklyn Law Review* staff for their hard work and support. Special thanks to my parents, Lou and Teri, my sisters, Elizabeth and Vivian, and my family and friends for their encouragement during the writing process.