THE GDPR'S LOSE-LOSE DILEMMA: MINIMAL BENEFITS TO DATA PRIVACY & SIGNIFICANT BURDENS ON BUSINESS

SARAH SHYY*

TABLE OF CONTENTS

INTRODUCTION

For each of its billions of users, Google collects every search query and website visited using Google Search; every location visited in Google Maps; every

email sent through Gmail; every video watched on YouTube; every detail submitted on a form using Google Chrome; every day-to-day activity of Android users; and more.[1] Google, alongside most businesses online, collects massive quantities of consumer data. Billions of data points exist, covering nearly every U.S. consumer.[2] This data often includes sensitive information, such as names, addresses, net worth, political preferences, and health information.[3]

Until recently, U.S. companies were free to exploit this data in the absence of comprehensive U.S. federal data privacy laws. Privacy policy agreements, as enforced by the Federal Trade Commission ("FTC"), afforded some protections; however, this self-regulating framework repeatedly fails to protect consumer privacy.[4] Companies fail to adequately inform consumers of their data collection practices, misuse data, and lack proper security measures to prevent major data breaches.[5] Recently, Facebook revealed that over 87 million Facebook users' data was leaked to Cambridge Analytica, a data analytics firm, and used to create profiles of American voters that aided political campaigns.[6] This breach led to widespread outrage and increased concerns over the collection and use of users' data.[7]

Despite the outrage, U.S. legislatures have struggled to pass any comprehensive federal privacy regulation that governs the collection of consumer data. Many argue that the current privacy policy regime fails to protect consumers.[8] Others argue that excessive privacy regulation may hamper businesses and innovation.[9] After years of debate and multiple failed proposals, no consensus has

---

*J.D. Candidate, May 2020, Loyola Law School, Los Angeles; B.A. Legal Studies, University of California, Berkeley, 2016. Special thanks to Professor Jennifer Rothman for her guidance throughout the writing process and to the members of UC Davis's Business Law Journal for their editorial revisions.

1 DOUGLAS SCHMIDT, GOOGLE DATA COLLECTION, DIGITAL CONTENT NEXT 1, 3, 8, 11, 26-27, 29 (2018).

2 EDITH RAMIREZ ET AL., FED. TRADE COMM'N, DATA BROKERS A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 46 (2014).

3 *Id.* at B-3.

4 *See* GINA STEVENS, CONG. RES. SERV., PRIVACY PROTECTIONS FOR PERSONAL INFORMATION ONLINE 1, 3 (2011).

5 *See, e.g.*, Philip Howard & Kris Erickson, *Data Collection and Leakage*, 84 CHI.-KENT L. REV. 737, 739-742 (2010) (describing how data is collected, often misinterpreted, and massively leaked in the context of political consumer data).

6 Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

7 *Id.*

8 Angelique Carson, *At US House hearing: It's not if a federal privacy bill should pass, but what it should contain*, INT'L ASS'N OF PRIVACY PROF'LS (Feb. 27, 2019), https://iapp.org/news/a/at-house-hearing-its-not-if-a-federal-privacy-bill-should-pass-but-what-it-should-contain/.

9 *Id.*

been reached.[10] U.S. lawmakers, now more than ever, are looking at other approaches to data privacy regulation, particularly the General Data Protection Regulation ("GDPR").[11]

The GDPR regulates data protection and privacy in the EU.[12] The EU legislators' goal was two-fold: to strengthen individuals' rights and to make it easier for EU companies to conduct business by harmonizing all Member States' data protection laws.[13] The GDPR gave consumers new rights including a right to notice, a right to access data collected, and a right to erase data upon request.[14] Notably, the GDPR applies to companies of all sizes, big and small, that process data.[15]

However, many scholars highlight that the GDPR fails to promote consumer privacy because consumers are still heavily pressured to agree to companies' data collection practices.[16] Gmail, Facebook, and most companies online *require* users to agree to their privacy policies in order to access their services.[17] In effect, if a consumer chooses to opt-out of a company's data collection practice, that consumer is then denied access to the company's service. With most companies utilizing "opt-in" requirements[18] and with society's increasing reliance on the Internet, consumers lack the time, money, and resources to choose to opt-out of data collection practices. As a result, consumers lack

---

[10] MÜGE FAZLIOGLU, INT'L ASS'N OF PRIVACY PROF'LS, CONSENSUS AND CONTROVERSY IN THE DEBATE OVER FEDERAL DATA PRIVACY LEGISLATION IN THE UNITED STATES 2-7 (2019), https://iapp.org/media/pdf/IAPP_US_Federal_Data_Privacy_Legislation_WhitePaper.pdf

[11] Elizabeth Schulze, *The US wants to copy Europe's strict data privacy law – but only some of it*, CNBC (May 23, 2019), https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html.

[12] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation"), L119/2 par. 6, 2016 O.J. (L 119) [hereinafter *General Data Protection Regulation*].

[13] *Questions and Answers – General Data Protection Regulation*, EUR. COMM'N (Jan. 24, 2018), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 [hereinafter *Questions and Answers*].

[14] *General Data Protection Regulation, supra* note 12, at art. 7, 15, 17.

[15] *Id.* at art. 2.

[16] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013); Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 390 (2013).

[17] *See, e.g.*, *Create a New Account It's Quick and Easy*, FACEBOOK, http://facebook.com (last visited Feb. 26, 2020) ("By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time."); *Sign up to see photos and videos from your friends*, INSTAGRAM, https://www.instagram.com/accounts/emailsignup/ (last visited Feb. 26, 2020) ("By signing up, you agree to our Terms , Data Policy and Cookies Policy"); *Sign Up to Ride*, UBER, https://auth.uber.com/login/?uber_client_name=riderSignUp (last visited Feb. 26, 2020) ("By clicking 'Sign Up', you agree to Uber's Terms of Use and acknowledge you have read the Privacy Policy.").

[18] *Id.*

meaningful choice to opt-out of data collection practices because "opting-out" is too costly. Daniel Solove emphasizes that "privacy self-management" frameworks like the GDPR, where consumers must proactively assert their rights, create an illusion of protecting privacy.[19] Consumers still lack the ability to make free, informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of personal data, and there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity.[20]

Meanwhile, the GDPR has imposed high implementation and compliance costs on businesses of all sizes. While predominant players like Google and Facebook have the resources to implement the GDPR's costly mandates, the GDPR places a particularly high burden on small to medium sized businesses ("SMCs"). This Article refers to SMCs as those employing less than 1000 employees, and this number is relative to corporate giants like Google, Amazon, and Facebook, which collectively employ hundreds of thousands of employees. Many new startups have neither steady revenue streams nor profitability.[21] In addition, the GDPR deprives SMCs of business, many companies have migrated to larger players that have dominated the data privacy realm because European courts have ruled that any part of the Internet ecosystem, including third party chipmakers, component suppliers, and software vendors that have never interacted with consumers, can also be liable for data breaches.[22] Moreover, many SMCs have decided to stop doing business in the EU because the cost of doing business is too high.[23]

This Article examines whether the benefits to consumer privacy that the GDPR produces outweigh the significant costs that the GDPR places on SMCs. I conclude that the GDPR provides only minimal benefits to consumer privacy that fail to justify the significant burden placed on SMCs. Accordingly, when the federal government and individual states within the United States consider adopting their own privacy legislation, they should consider the failings of the GDPR and design privacy legislation that is both more effective and less burdensome.

This Article proceeds in five parts. Part I provides an overview of online data collection. Part II provides an overview of the EU's GDPR. Part III outlines the framework that this Article uses to compare the benefits to consumer privacy

---

19 Solove, *supra* note 16.

20 *Id*. at 1885-86.

21 *See* Elizabeth Pollman, *Start-up Governance*, 168 U. PA. L. REV. 155, 170-76 (2019) (discussing the complexity of the capital structures of startups).

22 *The 10 Problems of the GDPR The US can learn from the EU's mistakes and leapfrog its policy: Hearing on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation Before the S. Judiciary Comm.*, 116th Cong. 5 (2019) (statement of Roslyn Layton, visiting scholar, American Enterprise Institute) [hereinafter *10 Problems of the GDPR*].

23 *Id.*

and burdens on SMCs that the GDPR produced. Part IV analyzes whether the GDPR has, in fact, achieved greater consumer privacy and whether the GDPR has imposed significant costs on mid-size businesses. Part V highlights the need for more effective and less burdensome data privacy regulation than the GDPR, and it recommends adopting principles like "privacy by design and default."

I. THE LACK OF ONLINE DATA PRIVACY

This section provides an overview of online data collection, the U.S.'s ad hoc approach to data privacy regulation, and the problems that arise from consumer data usage. By doing so, this section aims to highlight the need for some type of data privacy regulation and later aims to explore whether the GDPR has, in fact, dealt with these issues.

A. What is Online Data Collection?

Consumer brands in virtually every industry collect data on their consumers.[24] Companies gather data by monitoring online activities such as websites visited, search queries, and information shared online.[25] Data is also gathered indirectly by tracking consumers' physical location and mobile application use through mobile devices when users are offline. [26] The type of data collected is far-reaching. Data brokers collect billions of data points on consumers that often include sensitive information such as their name, address, social security number, driver's license number, race & ethnicity, occupation, judgments, bankruptcies, social media accounts, home loans, types of credit cards, vehicles owned, travel purchases, and buying activity.[27]

Businesses collect data because it is lucrative, so much so that data is often referred to as the "new oil."[28] Data is often sold to third-parties like data brokerage firms that buy, analyze, and sell data. These firms collect and store data on almost *every* U.S. consumer.[29] They categorize consumers into categories, like "single mom struggling in urban setting," "people who do not speak English and feel more comfortable speaking in Spanish," and "gamblers."[30] This information is then sold

---

[24] *How to think about data in 2019*, ECONOMIST (Dec. 22, 2018), https://www.economist.com/leaders/2018/12/22/how-to-think-about-data-in-2019 [hereinafter *How to think about data in 2019*].

[25] Carolyn Gray, *Who Pays the Price? Regulation of Data Tracking and Online Behavioral Advertising*, 8 ARIZ. SUMMIT L. REV. 385, 386-88 (2015).

[26] *Id.* at 388.

[27] RAMIREZ, *supra* note 2, at B-3.

[28] *The world's most valuable resource is no longer oil, but data,* ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[29] RAMIREZ, *supra* note 2, at iv.

[30] *Id.* at B-3.

to various companies like other data brokerage firms, advertising companies, and analytic firms that perform a variety of services.[31] This information is often used to determine the type of access people have to services. [32] Today, Uber ratings determine who gets a ride; Airbnb reviews decide what sort of property you can stay in; dating-app algorithms select potential life partners; location and payment history determines what products firms try to sell; and online searches sometimes even establishes prices.[33] Although some personal data is anonymized, much data is not and can easily be decoded to discern user identities.[34]

B. Online Data Privacy Protection in the U.S.

While the EU implemented the GDPR, there is only a "patchwork" of federal regulations in the United States that protect certain types of sensitive information.[35] For instance, the Health Insurance Portability and Accountability Act protects the data regarding one's health and the Children's Online Privacy Protection Act protects the data of children under the age of thirteen.[36] However, there is no single, comprehensive federal regulation in the United States that regulates most of the data collected online.[37] Several states have also adopted various types of data privacy regulations such as medical record privacy laws that, in varying degrees, restrict access and disclosure of patient health information.[38]

Recently, California passed the California Consumer Privacy Act ("CCPA"), providing broad data privacy regulations. The CCPA applies to any business that earns $25 million in revenue per year, sells 50,000 consumer records per year, or derives 50% of its annual revenue from selling consumer's personal information.[39] Like the GDPR, companies must disclose and deliver personal

---

31 *Id.* at 7-9.

32 *How to think about data in 2019*, *supra* note 23.

33 *Id.*

34 *See, e.g.*, Daniel Kondor, Behrooz Hashemian, Yves-Alexandre de Montjoye, & Carlo Ratti, *Towards matching user mobility traces in large-scale datasets*, IEEE TRANSACTIONS ON BIG DATA (Aug. 14, 2018) (concluding that an agent could match user trajectories in anonymized data from one dataset with deanonymized data in another to unmask the anonymized data).

35 Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

36 *Id.*

37 *Id.*

38 *See, e.g.*, CAL. CIV. CODE § 56 (2019) (Confidentiality of Medical Information Act); JOY PRITTS ET AL., THE STATE OF HEALTH PRIVACY A SURVEY OF STATE HEALTH PRIVACY STATUTES VOL. 1 (2002), http://sharps.org/wp-content/uploads/PRITTS-REPORT1.pdf (providing a survey of each state's health privacy laws); JOY PRITTS ET AL., THE STATE OF HEALTH PRIVACY A SURVEY OF STATE HEALTH PRIVACY STATUTES VOL.2 (2002), https://cdt.org/files/pdfs/The%20State%20of%20Health%20Privacy%20(Volume%202).pdf (providing a survey of each state's health privacy laws).

39 CAL. CIV. CODE § 1798.140 (2019).

information collected upon request of the consumer.[40] Companies must inform consumers about what data is collected, for what purposes, and to whom it is sold.[41] Consumers are given a right to "opt-out" of the sale of their personal information.[42] Companies must also place on their homepage a clear and conspicuous link entitled "Do Not Sell My Personal Information" that directs consumers to a webpage that enables them to opt out of the sale of information.[43] Companies must delete consumer information that has been collected upon consumer request.[44] Companies are responsible for ensuring that employees are trained in handling consumer inquiries related to data privacy.[45] In cases of non-compliance, consumers can assert a private right of action against a company.[46] Statutory damages can range between $100 and $750 per consumer per incident or actual damages, injunctive relief, and any other relief the court deems proper.[47] The California Attorney General can enforce a penalty of up to $7,500 per incident.[48] Damages have the potential to reach millions considering that security breaches can result in the leak of millions of consumers' data.

Nevertheless, within this loose framework of data privacy laws, companies continue to self-regulate their collection practices through privacy policy agreements. A privacy policy is a written description on a website explaining to the public how the company applies fair information practices to the collection, use, storage, and dissemination of personal information provided by users.[49] Users are presented these privacy policies and given the opportunity, often through clicking on an "I Agree" button, to accept the terms.[50] In essence, companies rely on a framework of notice and consent to collect data. These terms include what data is collected, why it is collected, and how the data is used.[51]

The FTC, an agency tasked with protecting consumers, relies on Section 5 of the Federal Trade Commission Act ("FTC Act") to hold companies to these agreements. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[52] The FTC characterizes violations of privacy

---

40 *Id.* § 1798.130.
41 *Id.* § 1798.115.
42 *Id.* § 1798.120(a).
43 *Id.* § 1798.135.
44 *Id.* § 1798.105.
45 *Id.* § 1798.130.
46 *Id.* § 1798.150.
47 *Id.*
48 *Id.* § 1798.155.
49 STEVENS, *supra* note 4.
50 Sloan & Warner, *supra* note 16 at 373-74.
51 *See, e.g.*, *Data Policy*, FACEBOOK (Apr. 19, 2018), https://www.facebook.com/policy.php; *Google Privacy Policy*, GOOGLE (Jan. 22, 2019), https://policies.google.com/privacy?hl=en#intro; *Microsoft Privacy Statement*, MICROSOFT (Nov. 2018), https://privacy.microsoft.com/en-us/privacystatement.
52 15 U.S.C. § 45 (2018).

policies as "unfair" and "deceptive" trade practices. For instance, the FTC reached a settlement with Lenovo after claiming Lenovo's failure to disclose that one of its programs collected and transmitted consumer Internet browsing data to a company that delivered pop-up ads was an unfair and deceptive practice.[53] Additionally, the FTC has also used Section 5 to address data security, forcing multiple companies into settlements where the companies "put consumers' personal data at unreasonable risk."[54] For example, the FTC settled a complaint with Uber alleging Uber deceived consumers by failing to reasonably secure sensitive consumer data stored in the cloud.[55] Nevertheless, under current federal privacy laws, companies set the scope of their privacy policies. As firms increasingly gather and disseminate intimate details of consumers' lives, the concern for consumer privacy and security also increase.

C. Problems with Online Data Collection

In the absence of comprehensive federal data privacy regulation, privacy policies fail to adequately inform users of data collection practices, data is misused, and security vulnerabilities threaten consumer privacy. This section summarizes the issues surrounding consumer privacy in order to examine whether the GDPR provides an adequate solution.

1. Lack of Notice

Companies have thus far failed to inform consumers about the type of information collected, how that information is used, and whom that information is shared with. A user's consent is informed if the user has "sufficient knowledge of the practices to make a reasonable evaluation of the risks and benefits of disclosing information."[56] However, Richard Warner and Robert Sloan emphasize that informed consent is impossible because data collection systems are so complex, stating "any attempt to trace what information is collected, the purposes for which it is used, and where it goes is 'so complicated that probably only a handful of deep experts would be able to piece together a full account."[57] Solon Barocas and Helen Nissenbaum explain that this complexity stems, in part, from data collection's

---

[53] In the Matter of Lenovo (United States) Inc., F.T.C. File No., Dock. No C-4636, 152 3134 (Dec. 20, 2017).

[54] Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN. ST. L. REV. 777, 790 (2016).

[55] In the Matter of Uber Tech. Inc. Complaint, F.T.C. File No. 1523054 (Aug. 15, 2017); Decision and Order, F.T.C. File No. 1523054, (Aug. 15, 2017); Agreement Containing Consent Order, F.T.C. File No. 1523054, (Aug. 15, 2017).

[56] Warner & Sloan, *supra* note 16.

[57] *Id.* at 393 (quoting Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DÆDALUS 32, 35 (2011)).

constantly evolving landscape as "new companies bloom, novel analytical tools emerge, business relationships begin and end."[58]

As a result, privacy policies are extremely cumbersome to read. A 2008 study revealed that it takes approximately 201 hours a year to read all the privacy policy agreements encountered in a year.[59] That amount of time has likely increased over the decade, given the growth in number and diversity of websites, as well as the GDPR-related updates creating longer policies.[60] Policies contain complex legalese that is difficult for the average reader to understand.[61] Many companies also intentionally include broad language to grant greater flexibility.[62] One survey revealed that a mere 34% of firms collecting data felt their organizations were "very effective" at being transparent with customers about how data is used and 9% of firms felt their organizations are "totally ineffective" at transparency.[63]

The practice of sharing data with third-parties, particularly data brokers, exacerbates the problem. Consumers are largely unaware that data brokers are collecting and using information because data brokers do not obtain information directly from consumers.[64] The endless chain of sharing information from data broker to data broker makes it extremely difficult for consumers to track their data.[65] Altogether, businesses have failed to adequately inform users of their data collection practices.

---

58 SOLON BAROCAS & HELEN NISSENBAUM, ON NOTICE: THE TROUBLE WITH NOTICE AND CONSENT (2009).

59 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 565 (2008).

60 Alexis C. Madrigal, *Reading the Privacy Policies You Encounter Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

61 *See* Kevin Litman-Navarro, *We Read 150 Privacy Polices. They Were an Incomprehensible Disaster.,* N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html ("Only Immanuel Kant's famously difficult 'Critique of Pure Reason' registers a more challenging readability score than Facebook's privacy policy.").

62 *See* LESLEY SZANTO FRIEDMAN & CLAUDINE MEREDITH-GOUJON, PAUL, WEISS, RIFKIND, WHARTON & GARRISON, REVISING PRIVACY POLICIES ON THE INTERNET 3 (2001), https://www.paulweiss.com/media/1953327/16716.pdf (discussing the benefits of revising broadly protective language in an existing privacy policy to help dispel concerns that the company is trying to expand its use of consumer information).

63 ECONOMIST INTELLIGENCE UNIT, THE BUSINESS OF DATA 4 (2015), https://eiuperspectives.economist.com/sites/default/files/images/Business%20of%20Data%20briefing%20paper%20WEB.pdf.

64 RAMIREZ, *supra* note 2, at 46.

65 *Id.*

2. Misuse of Data

The data collected is often used in ways that are not in the consumers' interest. Ari Waldman reveals that social networking companies, like Facebook, leverage consumer trust in their network of friends to manipulate consumers into sharing more information.[66] Cambridge Analytica, a data analytics firm, was able to harvest fifty million Facebook profiles and use that data to target American voters during the 2016 election.[67] Many consumers are also opposed to targeted advertisements that are often based on incorrect assumptions.[68] According to the Pew Research Center, "[a]bout two-thirds (68%) of internet users disapproved of search engines and websites tracking their online behavior in order to aim targeted ads."[69] Targeted ads and other artificial intelligence features often rely on opaque, skewed information that facilitate discrimination and constrain consumer options.[70] One of Facebook's advertising features allowed advertisers to exclude specific groups referred to as "Ethnic Affinities" and, in effect, allowed advertisers to exclude users based on race, gender, and other sensitive factors.[71] Consumers are denied credit because of inaccurate predictions based on arbitrary facts like "a consumer's friends, neighbors, and people with similar interest, income levels, and backgrounds."[72] In sum, data usage ranges from unwanted targeted ads, the sale of information to lenders who could then use the information to deny consumers credit or employment, to actual discrimination on the basis of race and other protected classes.[73]

---

[66] Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193, 221-25 (2016).

[67] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[68] Chris Dobson, *Targeted Advertising Requires Good Data*, FORBES (Apr. 5, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/04/05/targeted-advertising-requires-good-data/#5e4d7f3a29db ("Machine learning alone, however, cannot offer accurate intelligence for all marketing efforts—data discrepancies have been plaguing the industry for years and we still don't seem to be any further forward.").

[69] Russell Heimlich, *Internet Users Don't like Targeted Ads*, PEW RES. CTR. (Mar. 13, 2012), http://www.pewresearch.org/fact-tank/2012/03/13/internet-users-dont-like-targeted-ads/.

[70] *See* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 88-98 (2019).

[71] *Id.* at 80; Michelle Geronimo, *Online Browsing: Can, Should, and May Companies Combine Online and Offline Data to Learn about You*, 9 HASTINGS SCI. & TECH. L.J. 211, 223 (2017).

[72] Matthew A. Bruckner, *The Promise and Perils of Algorithmic Lenders' Use of Big Data*, 93 CHI.-KENT L. REV. 3, 25-29 (2018); Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE J. L. & TECH. 148, 151-152 (2016).

[73] JUSTIN BROOKMAN & G.S. HANS, WHY COLLECTION MATTERS SURVEILLANCE AS A DE FACTO PRIVACY HARM 3 (2013), https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.

Companies often violate their own privacy agreements with customers. For instance, Google initially allowed consumers to choose whether to "check out" its new product, Google Buzz social networking program.[74] However, some people who opted not to be included in Buzz were enrolled anyways and their data was transferred from Gmail accounts to Google Buzz.[75] While the FTC discovered and acted on this violation, the FTC's reach is extremely limited without clear guidelines and resources to regulate all U.S. companies. Joel Reidenberg points out that "[n]otice and choice cannot resolve the failure of a website to adhere to the terms of the notice."[76]

3. Security Issues

Online data collection also creates greater risk of security hazards for consumers. Companies routinely experience data breaches as a result of both inadequate security measures and aggressive external hacking.[77] As a result, consumers are exposed to financial fraud, identity fraud, and inadvertent identification as hackers obtain personal information.[78] For instance, a cyberattack on Equifax, a consumer credit reporting agency that also aggregated online data, resulted in the compromising of 145.5 million Social Security numbers, more than 200,000 credit card numbers including expiration dates, and about 182,000 government-issued identification documents like driver's licenses, taxpayer ID cards, passports, and military IDs.[79] "Data breach could also reveal private, embarrassing information that a consumer did not want shared."[80] Unauthorized breaches have also occurred when employees and contractors who have unique access to the databases misuse or abuse their privileges. In one case, a Google engineer spied on the user accounts of multiple minors, viewing their contact lists, chat transcripts, and call logs, and used the information to manipulate those same users.[81] Recently, former Twitter employees were charged with spying for Saudi

---

74 Kathleen Ann Ruane, CONG. RESEARCH. SERV., RL34693, ONLINE DATA COLLECTION AND DISCLOSURE TO PRIVATE ENTITIES, 2 (2011).

75 *Id.*

76 Joel R. Reidenberg et. al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 ISJLP I/S: J.L. & POL'Y FOR INFO. SOC'Y 485, 521 (20145).

77 *See, e.g.*, Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have be stolen,* BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 ("Data breaches are becoming common for all kinds of businesses, including retailers. . . . Many of these breaches were caused by flaws in payment systems that were taken advantage of by hackers.").

78 BROOKMAN & HANS, *supra* note 72.

79 Equifax's Statement for the Record Regarding the Extent of the Cybersecurity Incident Announced on September 7, 2017, SEC. EXCHANGE COMM'N (Sept. 7, 2017), https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/d583804dex991.htm.

80 BROOKMAN & HANS, *supra* note 72, at 273.

81 *Id.* at 3.

Arabia by accessing over 6,000 Twitter accounts and providing personal information on dissidents who use the platform.[82] Schwartz and Solove also highlight that anonymized data can be combined to reveal personally identifiable information.[83] Reidenberg also points out that a notice and consent framework cannot be used to address problems with data security because it involves third-parties accessing information.[84]

Security threats are an issue even in the absence of data breach. Julie Cohen underscores that "[n]etworked information technologies enable surveillant [sic] attention to become continuous, pervasively distributed, and persistent."[85] As a result, people-search products that rely on the collection of online data can facilitate harassment and stalking.[86] Government access to these commercial databases without "robust due process protection" poses another significant threat to consumers.[87] As revealed during the NSA-Snowden affair, the government derives much of its data from commercial stores of data without transparent processes and without a particularized showing of suspicion.[88]

These data privacy issues have had dire consequences on consumer privacy and have led many U.S. consumers and legislators to push for data privacy regulation. The following section provides an overview of the EU's GDPR, which was enacted, in part, to combat many of these data privacy issues. While the EU's GDPR only applies to companies that do business in the EU, it is a good case example of the types of benefits and consequences that federal data privacy regulation can have if and when the U.S. adopts its own regulation.

II. THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

In contrast to the ad hoc U.S. response to online privacy issues, the European Union ("EU") has implemented a broad uniform standard to which it expects businesses with an online presence to conform to as a minimum standard of privacy protection. The GDPR imposes strict rules on controlling and processing

---

82 Ellen Nakashima & Greg Bensinger, *Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics*, WASH. POST (Nov. 6, 2019), https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html.

83 Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U.L. REV. 1814, 1841-45 (2011).

84 Joel R. Reidenberg et. al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 ISJLP 485, 522 (2015).

85 Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1915 (2013).

86 BROOKMAN & HANS, *supra* note 73.

87 *Id.* at 4.

88 *Id.*

personal identifiable information.[89] If an organization offers goods or services to, or monitors the behavior of EU residents, it must comply with the GDPR.[90] As such, many U.S. companies have had to comply with the GDPR's requirements.

A. Why was the GDPR implemented?

Prior to the GDPR's adoption, the Data Protection Directive 95/46/EC ("DPD") protected the personal data of EU citizens.[91] The DPD, enacted in 1995, sought to achieve a balance between "the protection of . . . the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other."[92] However, rapid growth in technology and globalization posed new challenges for data protection. Technology, such as social media and cloud computing, allows individuals to share information publicly and globally on an unprecedented scale, encouraging mass exploitation of consumer data and posing security threats on an unprecedented scale.[93]

The DPD's limited scope failed to address the data issues created by new technology and globalization created. One concern was the need to "clarify and specify the application of data protection principles to new technologies."[94] Another concern was the "lack of sufficient harmonization between Member States' legislation on data protection, in spite of a common EU legal framework."[95] An additional concern was that the increased outsourcing of processing, very often outside the EU, raised several problems in relation to the law applicable to the processing and the allocation of associated responsibility.[96] Others stressed the need for stronger institutional arrangement for the effective enforcement of data protection rules. [97]

To address these concerns, the European Commission, European Parliament, the Working Party of Article 29, and other stakeholders called to adopt a comprehensive approach on data protection to strengthen individuals' rights and

---

[89] Kris Lahiri, *What is General Data Protection Regulation?*, FORBES (Feb. 14, 2018), https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/#7b93750562dd.

[90] *Id.*

[91] Commission Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995 O.J. (L 281) 31.

[92] EUR. COMM'N, A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION (2010).

[93] *Id*.

[94] *Id*. at 3.

[95] *Id*.

[96] *Id*. at 4.

[97] *Id*.

enhance the internal market dimension.[98] On the individual rights' front, the European Commission called for providing protection for individuals in all circumstances, increasing transparency for data subjects, enhancing control over one's own data, raising awareness, ensuring informed and free consent, protecting sensitive data, and making remedies and sanctions more effective.[99] On the internal market dimension front, the European Commission called for increasing legal certainty and providing a level playing field for data controllers through harmonization of laws, reducing the administrative burden through revision and simplification, clarifying the rules on applicable law and Member States' responsibility, and enhancing data controller responsibility through effective policies and mechanism to ensure compliance, and encouraging self-regulatory initiatives.[100]

Looking to reform the legal framework, many emphasized the importance of securing consumer trust and generating growth in the EU market. Viviane Reding, the EU's Justice Commissioner, stated:

> European businesses need to take advantage of this new computing and information-sharing landscape and European consumers need to be able to navigate safely though the digital age. A uniform and modern data protection law for the European Union is exactly what we need to secure trust and generate growth in the digital single market.[101]

In the DPD's place, the GDPR sought to accomplish these overarching goals, but as examined later, the GDPR falls short in doing so. The following section provides a brief overview of the GDPR.

B. Overview of the GDPR

The GDPR enacted an extensive list of requirements.[102] The GDPR's main components include: an increased territorial scope, strict processing requirements,

---

[98] *Id.*; EUR. DATA PROT. SUPERVISOR, OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR: A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION (2011); ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND DETERMINING WHETHER PROCESSING IS "LIKELY TO RESULT IN A HIGH RISK" FOR THE PURPOSES OF REGULATION 2016/679 (2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[99] *Id.*

[100] EUR. COMM'N, A COMPREHENSIVE APPROACH, *supra* note 91.

[101] Press Release, Eur. Comm'n, European Data Protection Day 2013: Full Speed ahead towards reliable and modern EU data protection laws (Jan. 28, 2013), https://ec.europa.eu/commission/presscorner/detail/en/IP_13_57 [hereinafter Press Release: Eur. Data Protection Day 2013].

[102] *General Data Protection Regulation*, *supra* note 12.

new data subject rights,[103] mandated security protocols, and accountability.[104] The following sections provide brief overviews, EU case illustrations, and various scholarly critiques on each of these components.

1. Territorial Scope

The GDPR expanded its scope beyond the EU Member States. Article 3 broadly provides that all companies that process EU citizen's data are subject to the GDPR "if processing is related to: (1) the offering of goods or services to data subjects in the EU (even if no payment is required for such goods or services); or (2) monitoring the behavior of the data subjects provided that such behavior takes place in the EU."[105] Companies processing EU consumer data must comply, "regardless of whether the processing takes place in the Union or not."[106] As a result, the GDPR affects many U.S. companies that provide services to EU residents. Some criticize the extraterritorial effect by characterizing it as "regulatory overreach" and "intrusion on state sovereignty."[107] However, others argue that international law and custom allow such reach and many countries have enacted similar extraterritorial regulations such as U.S. antitrust laws.[108]

2. Strict Processing Requirements

The GDPR requires that data collection must be "processed lawfully, fairly, and in a transparent manner in relation to the data subject."[109] This includes that requests for consent must be given in an "intelligible and easily accessible form, using clear and plain language," and it must be "freely given."[110]The GDPR requires that data collection must be "processed lawfully, fairly, and in a transparent manner in relation to the data subject."[111] This includes that requests for consent must be given in an "intelligible and easily accessible form, using clear

---

[103] *Id.* at art. 4 (defining "data subjects" as any person whose personal data is collected, held, or processed).

[104] *See also* Kimberly A. Houser & Gregory Voss*, GDPR: The End of Google and Facebook Or a New Paradigm in Data Privacy*, 25 RICH. J.L. & TECH. 1 (2018) (providing a comprehensive overview of the GDPR's main components along with examples of DPA enforcement cases against Google and Facebook).

[105] *General Data Protection Regulation*, *supra* note 12 at art. 3.

[106] *Id*.

[107] Houser & Voss*, supra* note 104, at 67-68 n.304.

[108] *Id*. at 68; Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L L. 53, 78-79 (2014).

[109] *General Data Protection Regulation*, *supra* note 12, at art. 5, sec. 1(a).

[110] *Id.* at art. 7, sec. 2, 4.

[111] *Id*. at art. 5, sec. 1(a).

and plain language," and it must be "freely given."[112] In France, Google was fined 50 million euros, roughly $54,949,250 as of February 26, 2020, for lack of transparency after France's watchdog found that users were not able to fully understand the extent of Google's processing and that Google's terms were too generic and vague.[113] The watchdog found, amongst other instances, that the language, "[t]he information we collect is used to improve the services offered to all our users. . . . The information that we collect and how we use them depends on how you use our services and how you manage your privacy settings," were too generic in light of the scope of the processing implemented and its consequences.[114] Google was also fined for lack of valid consent after Google automatically ticked the options for ad personalization and bundled consent for all products.[115] Discussed in greater detail in Section IV, many critics argue that "transparency" is impossible with machine learning and artificial intelligence.[116]

The GDPR also calls for data minimization, which requires limiting the collection of personal information to information that is directly relevant and necessary to accomplish a clear, specified purpose.[117] The collection of personal data revealing "sensitive" information, like race, political opinions, religious beliefs, is lawful only in narrow circumstances.[118] In practice, companies may only collect and store the data that they need and must delete everything else.[119] This requires companies to understand the data's context, such as development and testing, production, or data warehousing and analytics, and only collect, store, and use data within that context.[120] Some scholars argue that data minimization impedes growth and innovation by preventing "Big Data" initiatives from analyzing existing data.[121] This argument relies on the premise that, in theory, "with more data will come greater knowledge."[122]

---

112 *Id.* at art. 7, sec. 2, 4.

113 *Délibération n°SAN-2019-001 du 21 janvier 2019* [Deliberation No. SAN-2019-001 of 21 January 2019], COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS [National Commission of Computing and Freedoms], Jan. 21, 2019.

114 *Id*. at 16, par. 112.

115 *Id*. at 22-23.

116 Solove, *supra* note 16.

117 Bernard Marr, *Why Data Minimization Is An Important Concept In the Age of Big Data*, FORBES (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data.

118 *General Data Protection Regulation*, *supra* note 12, at art. 9.

119 Marr, *supra* note 117.

120 JT Sison, *Data Minimization in the GDPR: A Primer,* DATAGUISE (Feb. 15, 2017), https://www.dataguise.com/gdpr-compliance-data-minimization-use-purpose/.

121 Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1001 (2017).

122 *Id*.

3. Data Subject Rights

Under the right of access, "[t]he data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and . . . access to the personal data."[123] Data subjects are also given a right to access the purposes of the processing, the categories of personal data concerned, the recipients to whom the personal data will be disclosed, and the period for which data will be stored.[124] In Austria, YouTube, Amazon, Spotify, and other streaming services were served with complaints alleging that they either failed to respond to inquiries requesting personal data or provided raw data that was incomplete or incomprehensible.[125] Consumers also have the right to receive the personal data collected and transfer their data to other companies upon request.[126] Many scholars characterize this so-called 'right to explanation' as impossible for machine learning systems, as they rely on hundreds of thousands of variables that often lack any convenient or clear human interpretation.[127]

Additionally, companies must rectify "inaccurate personal data concerning [the data subject]" upon request.[128] Similarly, the right to be forgotten requires companies to erase personal data concerning a consumer when consent is withdrawn.[129] In *Google v. Spain*, the European Court of Justice ("ECJ") held that Europeans have a right, in some circumstances, to request search engines to remove links to their personal information because the data subject's rights override both the economic interest of the search engine and the interest of the general public in finding that information.[130] Many scholars argue that these rights pose First Amendment concerns.[131] Eugene Volokh explains, "[t]he difficulty is that the right to information privacy—the right to control other people's communication of personally identifiable information about you—is a right to have the government stop people from speaking about you."[132]

---

123 *General Data Protection Regulation*, *supra* note 12, at art. 15.

124 *Id*.

125 *Netflix, Spotify & Youtube: Eight Strategic Complaints filed on "Right to Access"*, NOYB: NOYB BLOG (Jan. 18, 2019), https://noyb.eu/access_streaming/.

126 *General Data Protection Regulation*, *supra* note 12, at art. 20.

127 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, 59 (2017).

128 *General Data Protection Regulation*, *supra* note 12, at art. 16.

129 *Id.* at art. 17.

130 Case C-132/12, *Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, 2014 ECLI:EU:C:2014:317 (May 13, 2014).

131 Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1050-51 (1999).

132 *Id*.

4. Data Security

The GDPR compels the practice of data protection by design and default. Article 25 of the GDPR requires companies "at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical data-protection principles … in an effective manner and to integrate the necessary safeguards into the processing."[133] This mandates implementing, at the earliest stages of the design of processing options, protective measures like pseudonymization and encryption of personal data.[134] Many scholars have argued that anonymization of data is a myth because large data sets and highly unique data could easily re-identify someone.[135]

Article 25 also requires companies to implement "appropriate technical and organisational [sic] measures for ensuring that, by default, only personal data necessary for each specific purpose of the processing are processed."[136] For example, "[a] social media platform should be encouraged to set users' profile setting in the most privacy-friendly setting by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons." [137] For ventures that carry "high risk" to the rights and freedoms of individuals companies must carry out an assessment of the impact of the operations on the protection of personal data and, if there is a "high risk," they must consult supervisory authority.[138] Examples of processing that carry a "high risk" include: profiling and predictive processing, automated-decision making that has legal effects, systematic monitoring, the processing of sensitive data, and processing that relies on new technologies.[139] Yet, the implementation of these security protocols are primarily outsourced to engineers, and Ari Waldman argues that this "automation of privacy law compliance to engineers at third-party vendors is threatening to replace real pro-consumer progress with mere *symbols of compliance*, undermining the promise of pro-privacy laws."[140]

Under Article 25, A German social network operator was fined 20,000 euros for failing to secure data after hackers stole passwords that were kept in plain

---

133 *General Data Protection Regulation*, *supra* note 12, at art. 25.

134 *What does data protection 'by design' and 'by default' mean?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (last visited Mar. 17, 2020) [hereinafter *What does 'by design' and 'by default' mean*].

135 Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 712-14 (2016).

136 *General Data Protection Regulation*, *supra* note 12, at art. 25.

137 *What does 'by design' and 'by default' mean*, *supra* note 133.

138 *General Data Protection Regulation*, *supra* note 12, at art 35-36.

139 ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 97.

140 Ari Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. (forthcoming 2020).

text, unencrypted and unaltered.[141] The GDPR's high standards require companies to review their processing structure and to ensure that personal data is only used and accessed by third parties for necessary purposes. In Austria, a sport betting café was fined 5,280 euros after Austria's watchdog found that the café's video surveillance system, covering public streets and parking lots in front of the entrance, did not have adequate processing like logging operations and deleting personal image data recorded and was not limited to a necessary extent.[142]

5. Accountability

Lastly, the GDPR implements high accountability standards to ensure compliance. Each company must designate a representative in the Union.[143] Companies must appoint a data protection officer, who must be involved in all issues that relate to the protection of personal data.[144] If a breach occurs, companies are required to notify data subjects and appropriate authorities within 72 hours.[145] The Dutch DPA fined Uber 600,000 euros, roughly $659,775.00 as of February 28, 2020, for failing to report a data breach within 72 hours that resulted in unauthorized access to names, e-mails, addresses, and telephone numbers of customers and drivers.[146] The GDPR also levies a high price for non-compliance. For instance, firms face penalties up to 4% of the total worldwide annual turnover or 20 million euros.[147] In addition, "any person who has suffered material or non-material damage as a result of an infringement of this regulation shall have the right to receive compensation from the controller or processor for the damage suffered."[148]

6. Small Businesses & GDPR Compliance

The GDPR applies to all companies, regardless of size, that process data.[149] It is worth noting that the GDPR exempts small firms, employing less than 250

---

[141] LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO [LfDI Baden-Wuerttemberg imposed its first fine in Germany after the DS-GVO], LFDI BADEN-WÜRTTEMBERG (Nov. 22, 2018), https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/.22, 2018).

[142] *First Austrian Fine: CCTV Coverage – Summary*, EUR. DATA PROT. BOARD (Sept. 12, 2018), https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_en [hereinafter *First Austrian Fine*].

[143] *General Data Protection Regulation*, *supra* note 12, at art. 27.

[144] *Id.* at art. 37-38.

[145] *Id.* at art. 33-34.

[146] *Dutch DPA: fine for data breach Uber*, AUTORITEIT PERSOONSGEGEVENS (Nov. 27, 2018), https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber.

[147] *General Data Protection Regulation*, *supra* note 12, at art. 83.

[148] *Id.* at art. 82.

[149] *Id*. at art. 2.

employees, from its recordkeeping, data protection officer, and impact assessment requirements.[150] However, these exemptions are *extremely* limited. Small firms must maintain records if their processing threatens consumer's rights and freedoms, if their processing occurs on a regular basis, or if their processing includes special categories of "sensitive" data described in Article 9.[151] Small firms must appoint a data protection officer if they use targeted advertising or process data on genetics and health.[152] Small firms must also conduct impact assessments if they use new technologies, monitor publicly accessibly areas such as through CCTVs, implement automatic, systematic processing, or process sensitive biometric data.[153] Most companies fall into these categories of exceptions. German DPA fined a small shipping company 5,000 euros for failing to have an adequate processing contract and transmitting data to a third parties.[154] Austria DPA similarly fined a small establishment with a surveillance camera that recorded individuals who passed on a sidewalk.[155] Thus, small firms cannot evade liability and must comply.

III. THE GDPR & A COMPARATIVE FRAMEWORK

The European Commission emphasized that the GDPR aims both to protect consumers' fundamental privacy rights and to support businesses by strengthening the single internal EU market.[156] A "single internal EU market" refers to the EU as one territory without any regulatory obstacles or borders,[157] and in terms of the GDPR, is believed to stimulate competition and trade by creating a single, pan-European law for data protection, a "one-stop-shop" for businesses with one supervisory authority, a level playing field amongst EU and non-EU companies, and technological neutrality.[158] Little scholarship analyzes whether the GDPR has, in fact, achieved these primary goals. Thus, this Article seeks to compare the GDPR's effect on consumer privacy and businesses, particularly SMCs, through a cost-benefit analysis framework.

---

150 *Id.* at art. 30.
151 *Id.* at art. 9.
152 *Id*. at art. 37.
153 *Id*. at art. 35.
154 Steven Craig, *German data protection authorities issue fines in 75 cases for GDPR breaches*, A&L GOODBODY (May 22, 2019), https://www.irelandip.com/2019/05/articles/cyber-risk-data-privacy/german-data-protection-authorities-issue-fines-in-75-cases-for-gdpr-breaches/.
155 *First Austrian Fine*, *supra* note 141.
156 Eur. Comm'n, Press Release, European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws (Jan. 28, 2013), https://europa.eu/rapid/press-release_IP-13-57_en.htm.
157 *The European single market*, EUR. COMM'N, https://ec.europa.eu/growth/single-market_en (last visited Nov. 9, 2019).
158 *Questions and Answers*, *supra* note 13.

This analysis proceeds in two parts. First, it examines to what extent has the GDPR benefitted consumer privacy and to what extent has the GDPR burdened businesses. Then, it compares whether the benefits to consumer privacy justify the burdens placed on businesses. This Article finds that the GDPR is both *ineffective* in protecting consumer privacy and *burdensome* on businesses of all sizes. In regards to consumer privacy, the GDPR and its rights-based framework create a false illusion of privacy. In regards to businesses, the GDPR imposes substantial compliance costs for businesses of all sizes and, more alarmingly, pose distributive justice concerns by creating high barriers for SMCs in the market. The next section applies this comparative framework to the GDPR and explains these findings in greater detail.

IV. A COMPARISON OF THE GDPR'S IMPACT

The GDPR affected companies across the globe and, in theory, seemed to provide consumers with greater consumer privacy. Yet, the GDPR, in practice, creates a false illusion of consumer privacy and enacts cost-prohibitive measures that disadvantage SMCs in the market. This section applies the comparative framework outlined in Section III, highlighting the minimal benefits to consumers and significant burden on businesses that the GDPR created.

A. Minimal Benefit to Consumer Privacy

The GDPR creates a false illusion of consumer privacy. As outlined in Section II, the GDPR grants consumers various "data subject rights" such as a right to erasure[159] and a right to an explanation.[160] This framework rests on the premise that consumers are free to decide whether to assert or waive these rights. However, consumers do not have the ability to make free, informed choices about whether to consent to a companies' data usage and thereby whether to assert these rights. If a consumer decides to opt-out of data collection, consumers are denied the companies' services. Gmail, Facebook, Instagram, Uber, and other popular websites each require users to agree to its privacy policy to access its services.[161] Opting-out essentially means opting-out of using the Internet because most companies condition access on consent. Consumers have no choice but to consent to a companies' data collection practices because society–workplaces, schools, apartment buildings, restaurants, transportation–continues to increasingly rely on the Internet and consumers simply cannot afford to opt-out. Thus, the GDPR creates a false illusion of privacy. Companies are still free to collect vast amounts

---

159 *General Data Protection Regulation, supra* note 12, at art. 17.
160 *Id.* at art. 12-14.
161 *See* sources cited *supra* note 17.

of personal data because a consumer, who lacked meaningful choice to begin with, clicks an "I agree" button.

Many scholars have stressed this lack of meaningful choice. Paul Schwartz and Daniel Solove highlight that, "If a consumer wants to buy a product, read a website, subscribe to a magazine, use a service, and so on, the consumer can be forced either to surrender privacy or to go elsewhere. But when nearly all companies offer the same take-it-or-leave it approach, consumers desiring to protect their privacy have nowhere to turn."[162] Daniel Solove further emphasizes that the "privacy self-management" framework, where the law provides people with a set of rights to enable them to make decisions about how to manage their data, creates an illusion of protecting privacy.[163] He emphasis that, in reality, these set of rights are meaningless. People lack the ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of personal data, and there are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity.[164] Through a data-driven lens, scholars highlight that "[t]he sheer ubiquity of pressures for personal information, the variety of situations in which they occur, and the seeming lack of alternatives—all these things apparently conspire to create a sense that resistance is futile."[165] Through a user-resource lens, Lilian Edwards and Michael Veale highlight that "[i]ndividuals are mostly too time-poor, resource-poor, and lacking in the necessary expertise to meaningfully make use of these individual rights."[166] Lauren Willis emphasizes, "so long as the public understands privacy as a right of individuals 'to determine for themselves when, how, and to what extent information about them is communicated to others,' better forms of regulation will remain unimagined."[167]

Various GDPR provisions have also failed to adequately protect consumers. The GDPR's requirement of fully informed consent continues to rely on the inadequate pre-existing 'notice and consent' framework.[168] Despite the wave of GDPR-compliant, updated privacy policies, many consumers remain unaware of company's data collection practices. Succinctly put, "why would anyone read the terms of service when they don't feel as though they have a choice in the first place? It's not as though a user can call up Mark Zuckerberg and negotiate his or

---

[162] Memorandum from Paul M. Schwartz, U.C. Berkeley, & Daniel Solove, Geo. Wash. Univ., to NPLAN/BMSG Meeting on Digital Media and Marketing to Children (June 29-30, 2009), https://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf.

[163] Solove, *supra* note 16.

[164] *Id.* at 1885-86.

[165] Warner & Sloan, *supra* note 16 at 404.

[166] 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, 67 (2017).

[167] Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 133 (2014) (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).

[168] *General Data Protection Regulation, supra* note 12, at art. 7.

her own privacy policy.'"[169] Other scholars found that electronic contracting nudges human beings to behave like simple stimulus-response machines that automatically and mindlessly "click-to-consent."[170] Additionally, legal ambiguity surrounding the GDPR's "right of access" has made personal data more vulnerable. One scholar, in his study, impersonated his fiancée and, through various organization's right of access processes, was able to obtain his fiancée's social security number, previous home addresses, hotel logs, school grades, whether she had used online dating, and even her credit card numbers.[171] Further, the GDPR's "right to be forgotten" also poses a different type of threat–hampering free speech. Robert Post emphasized that the public sphere is "a field of intersubjective communicative action" and it would "collapse if individuals could at will withdraw from circulation information 'relating to' themselves because they have the right to 'control' such data."[172]

The lack of meaningful choice and the failure of various GDPR provisions present the same consent, abuse, and security issues that plague prior privacy frameworks. Despite the bombardment of updated privacy policies after the GDPR went into effect, EU residents have not reported a greater sense of trust online.[173] The GDPR has failed to achieve its primary goal of protecting consumer privacy rights. The next section demonstrates that the GDPR has also failed to support businesses.

B. The Burden on Small Businesses

The GDPR has disadvantaged SMCs by enacting cost prohibitive measures, impeding business growth, and triggering companies to discontinue services in the EU. These categories are interrelated, but each demonstrates a significant burden on SMCs. In contrast, corporate giants, like Google, Amazon, and Facebook, have ample resources to comply and have gained market dominance in the EU since the GDPR's enactment.

---

[169] *How Silicon Valley Puts the 'Con' in Consent*, N.Y. TIMES (Feb. 2, 2019), https://www.nytimes.com/2019/02/02/opinion/internet-facebook-google-consent.html.

[170] Brett Frischmann & Evan Selinger, *Engineering Humans with Contracts* (Cardozo Legal Studies Research Paper Series No. 493, 2016); *see also* CHRISTINE UTZ ET AL., (UN)INFORMED CONSENT: STUDYING GDPR CONSENT NOTICES IN THE FIELD (2019), https://arxiv.org/pdf/1909.02638.pdf (discussing how consumers interact with different designs of cookie pop-ups and how various design choices can nudge and influence people's privacy choices).

[171] JAMES PAVUR & CASEY KNERR, GDPARRRR: USING PRIVACY LAWS TO STEAL IDENTITIES (2019), https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf.

[172] Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right To Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 1051 (2018).

[173] Lucy Tesseras, *GDPR three months on: Most consumers feel no better off*, MARKETING WEEK (Aug. 24, 2018), https://www.marketingweek.com/gdpr-three-months-on/.

SMCs cannot afford the GDPR's high implementation and compliance costs. On average, a firm of 500 employees must spend $3 million to comply with the GDPR.[174] Several studies revealed that common initial compliance costs include: time and salary spent with personnel devising and executing compliance strategy, integration of new software for seeking and recording active consent, legal fees, and contract management software.[175] Other studies have pointed to costs such as, "continually updating the data map with new fields and business systems, communicating process changes with all employees involved, producing robust compliance logs, and staying current with regulation updates or changes, in addition to processing [data subject requests that come through."[176]

These costs have a huge impact on startups that have neither steady revenue streams nor profitability until several years after they have established their company.[177] Many founders "bootstrap" their own business using their own funds, and those of family and friends, to finance development efforts and early operations.[178] SMCs, especially ones in their infancy, cannot afford millions in GDPR compliance, and are hindered from growing their business. Indeed, nearly 1 in 5 companies, particularly less mature and large firms, feel full compliance is impossible.[179] In part, "the lingering uncertainty around the GDPR is one of the biggest impediments to compliance, with parts of it deliberately left vague" including, "[u]ndefined terms such as 'undue delay,' 'likelihood of (high) risk to rights and freedoms' and 'disproportionate effort.'"[180] This leaves many SMCs exposed to crippling liability.

The GDPR has also impeded SMC growth, especially for European technology startups. One study revealed that fewer people are interested in

---

174 *10 Problems of the GDPR, supra* note 21 at 4.

175 *See, e.g.*, Nick Eckert, *What Are the Real Costs of GDPR Compliance?*, GDPR365 (last modified Apr. 30, 2019), https://www.gdpr365.com/what-are-the-real-costs-of-gdpr-compliance/; Jonathon Fruchte, *Cost of GDPR Compliance for a Small Software Business*, MEDIUM: EXPECTED BEHAVIOR (Oct. 4, 2018), https://medium.com/expected-behavior/cost-of-gdpr-compliance-for-a-small-software-business-eb2b8b8e829; DATAGRAIL, THE AGE OF PRIVACY: THE COST OF CONTINUOUS COMPLIANCE 5 (2019), https://datagrail.io/downloads/GDPR-CCPA-cost-report.pdf.

176 DATAGRAIL, *supra* note 175, at 7.

177 *See* Elizabeth Pollman, *Startup Governance*, 168 U. PA. L. REV. 155, 168 (2019) (discussing the complexity of the capital structures of startups).

178 *Id.* at 170.

179 J. TREVOR HUGHS & ANGELA SAVERICE-ROHAN, IAPP-EY ANNUAL GOVERNANCE REPORT 2018, at 67 (2019), https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf.

180 THOMSON REUTERS, *Top five concerns with GDPR compliance*, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance (last visited Feb. 26 2020).

investing in companies that face strict privacy laws like the GDPR.[181] Moreover, many companies have migrated to larger players, such as Google, Facebook, and Amazon, that have excelled in implementing data privacy requirements as European courts have ruled that any part of the Internet ecosystem, including third-party chipmakers, component suppliers, and software vendors that have never interacted with consumers, can be liable for data breaches.[182] This refusal to do business with SMCs impedes SMC development because many successful SMCs rely on outsourcing their larger needs to third-parties.

Most significantly, many companies have chosen to stop doing business in the EU. If the U.S. adopts a GPP model of data privacy, many SMCs based in the U.S. will face a huge economic burden that they cannot evade and may shut down. Various U.S. companies, like Williams-Sonoma and Pottery Barn, have closed their online doors to EU citizens.[183] Drawbridge, an identity-management company, exited the EU and sold off its ad-tracking business.[184] Various U.S. newspapers, like the Los Angeles Times and the Chicago Tribune, have also shutdown EU resident's' access to their websites.[185] With most prominent nations beginning to roll out strict privacy laws, SMCs will lose a huge customer base. A study revealed that smaller AdTech vendors "significantly" lost their market share reach; meanwhile, Google was able to slightly increase its reach after the GDPR was implemented. [186] "For users this means that while the number of third parties asking for access to their data is decreasing, a tiny few are getting more of their data."[187]

These effects have negative repercussions on consumers. While discussing various pro-competition regulatory frameworks, Tim Wu emphasizes the dangers of "a poorly designed regime, or a market that, in fact, does not support a large number of competitors, may simply add a regulatory burden, without much benefit for consumers, competitors, or anyone at all."[188] The GDPR imitates these concerns by increasing monetary barriers to entry and even leading companies to exit the EU market. In the long run, consumers are deprived of the benefits these businesses provide and face the growing threat of monopolistic control. Seen through the e-

---

[181] Leonid Bershidsky, *Europe's Privacy Rules Are Having Unintended Consequences*, BLOOMBERG (Nov. 13, 2018, 10:00PM), https://www.bloomberg.com/opinion/articles/2018-11-14/facebook-and-google-aren-t-hurt-by-gdpr-but-smaller-firms-are.

[182] *10 Problems of the GDPR, supra* note 21 at 4, 5.

[183] *Id.* at 3.

[184] *Id.*

[185] *Id.* at 5.

[186] Björn Greif, *Study: Google is the biggest beneficiary of the GDPR*, CLIQZ (Oct. 10, 2018), https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

[187] *GDPR – What happened?*, CLIQZ (Sept. 3, 2018), https://whotracks.me/blog/gdpr-what-happened.html.

[188] Tim Wu, *Antitrust via Rulemaking: Competition Catalysts*, 16 COLO. TECH. L.J. 33, 62 (2017).

book market, Amazon's sheer size allowed them to employ "below-cost pricing" tactics, handicapping competitors like Barnes & Nobles and giving Amazon the opportunity to raise prices.[189] The most alarming part is that Amazon's rapid, constant price fluctuations and personalized pricing allow Amazon to do so without consumers even realizing.[190] In markets that already make it hard for competitors to grow, the GDPR has proved to be another obstacle that SMCs must navigate, and has failed to balance these obstacles with greater consumer protections.

One of the primary goals of enacting comprehensive legislation was to strengthen an internal EU market and level the playing field for business.[191] However, the exact opposite occurred. SMCs' inability to comply with the GDPR's onerous burdens has allowed corporate giants to gain market dominance. Altogether, this impact is a significant cost and presents distributive justice concerns by imposing an unfair burden on SMCs.[192] The next section briefly analogizes to the same burdens the CCPA imposes on SMCs in California.

C. The CCPA & Small Business Owners

Small businesses have similarly expressed concern about the CCPA. An impact assessment estimates that "smaller firms (<20 employees) will incur $50,000 in initial costs . . . , medium-sized firms (20-100 employees) incur an initial cost of $100,000 . . . , [and] medium/large firms (100-500 employees) incur an initial cost of $450,000."[193] Again, for many SMCs this can be pricey to implement. Many concerns reflect the same concerns of the GDPR, including "worries about new privacy regulations necessitating a complete overhaul that can't be handled without losing business"; "lack of budget to implement necessary changes forcing companies to simply go offline"; "concerns about new regulations impeding growth"; "fears of inability to start a business due to regulatory burden"; and "concerns that even if SMBs are not unfairly burdened, increased costs for larger tech companies will be passed on to the SMBs that rely on their services."[194] These concerns also echo in the federal arena as legislatures debate what level of

---

189 Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 756-57 (2017).

190 *Id*. at 762-63.

191 Press Release: Eur. Data Protection Day 2013, *supra* note 100.

192 *See* JOHN RAWLS, A THEORY OF JUSTICE 276 (1971) ("[A] just scheme gives each person his due: that is, it allots to each what he is entitled to as defined by the scheme itself. The principles of justice for institutions and individuals establish that doing this is fair.").

193 DAVID ROLAND-HOLST ET AL., CAL. DEP'T OF JUSTICE OFF. OF THE ATTORNEY GENERAL, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS 11 (2019).

194 Scott Ikeda, *Will New U.S. Privacy Regulations Be Too Expensive for Small Businesses?*, CPO MAGAZINE (Mar. 26, 2019), https://www.cpomagazine.com/data-protection/will-new-u-s-privacy-regulations-be-too-expensive-for-small-businesses/.

data privacy laws to implement.[195] The CCPA provides the same poor options that the GDPR currently leaves SMCs with, but with few benefits to consumers as the same issue of lack of meaningful choice exists in California. The next section examines whether the benefits to consumer outweigh these costs.

D. The Burdens Outweigh the Benefits

The GDPR's benefits to consumer privacy fail to justify the burdens placed on SMCs. The key to data privacy regulation is striking a balance between privacy and allowing room for robust competition and business development. The dilemma is two-fold. On the one hand, pervasive privacy issues like lack of notice, misuse, and security issues demonstrate a need for comprehensive privacy regulations. On the other hand, there is an interest in promoting fair competition in the marketplace and, thereby, avoiding excessively hindering competition or adopting rules that disadvantage particular types of businesses.

Yet, the GDPR has failed to achieve this balance. Consumers still have little control over their own personal data. The GDPR obscures the root of the problem – namely that consumers have no meaningful alternatives. Consumers have no choice but to consent to companies' data collection practices because there are no alternative options. Despite the wave of updated privacy policies, consent is still neither voluntary nor fully informed. This perpetuates the problems that plague the U.S. self-regulated framework today: consumers remain unaware of how their data is used, companies continue to collect excessive amounts of data, and several GDPR provisions have even increased security issues. Meanwhile, SMCs are burdened by cost prohibitive measures, impediments to growth, and, ultimately, the threat of closing down. In particular, startups, which have spurred many popular services today, face heightened barriers to entry. This impact not only affects SMCs, but also burdens consumers in the long run that are deprived of services and forced to pay heightened prices. Section V concludes by highlighting the need for both more effective and less burdensome data privacy than the GDPR's data privacy model.

V. THE GDPR'S LOSE-LOSE DILEMMA

The GDPR model of data privacy regulation presents a lose-lose situation for both consumers and businesses. The GDPR's framework of data subject rights is incompatible with current data collection practices where consumers lack meaningful alternatives and are forced to accept an online company's privacy

---

[195] Odia Kagan, *Congress Debates U.S. Privacy Legislation, Impact on Small Businesses, Vulnerable Citizens*, FOX ROTHSCHILD LLP (Feb. 27, 2019), https://dataprivacy.foxrothschild.com/2019/02/articles/california-consumer-privacy-act/congress-debates-u-s-privacy-legislation-impact-on-small-businesses-vulnerable-citizens/.

policy. The GDPR's cost-prohibitive measures heavily burden businesses large and small, but, even more alarming, the measures pose particular distributive justice concerns by unfairly disadvantaging SMCs in the market. Thus, the GDPR has failed to benefit consumers in a manner that justifies the burdens placed on businesses.

Rather than copying the GDPR model, U.S. lawmakers should learn from the GDPR's failings and adopt regulation that is both more effective in protecting consumer privacy and less burdensome on businesses. The key question becomes what privacy regulations are both more effective and less burdensome. Data privacy by design and default presents one potential solution. Privacy by design and default bakes in privacy protections because the principle does not rely on consumers to proactively assert their rights. Instead, "privacy by design is a systematic approach to designing any technology that *embeds* privacy into the underlying specifications or architecture."[196] Privacy by design and default is less burdensome on SMCs because it tailors the amount of privacy protections to a company's data collection practices. SMCs that process small amounts of data do not have to spend millions of dollars to comply. Although privacy by design and default presents its own issues, it is beyond the scope of this Article to present a tried and true mechanism for more effective and less burdensome regulation. Instead, it compels U.S. lawmakers to consider the GDPR's failings and implement something better.

CONCLUSION

Today, federal U.S. lawmakers are rushing to adopt data privacy laws because of surmounting data privacy issues and new data privacy legislation arising across the globe. However, the GDPR fails to promote consumer privacy because, in today's data collection practices, consumers are forced to agree to a companies' data collection practices. Meanwhile, the GDPR has disadvantaged SMCs by imposing cost-prohibitive measures, hindering SMCs growth, and spurring SMCs to exit the market. The GDPR created a lose-lose dilemma for both consumers and businesses. U.S. lawmakers are urged to consider these failings and adopt legislation that is both more effective in protecting consumer privacy rights and less burdensome on businesses than the GDPR. Privacy by design and default demonstrates that this can be done. Ultimately, the focus of privacy regulation must shift from the outdated self-regulating model towards modern approaches that take into consideration today's realities.

---

[196] Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1412 (2011).

#TRADEMARKBULLY… *WHO ME*? A PRACTICAL GUIDE FOR ATTORNEYS ON HOW TO AVOID THE LABEL

PAUL MARTELLO*

Being called a #trademarkbully on social media happens and can be very problematic for trademark owners. However, certain cease and desist letters are effective at avoiding the #trademarkbully label and others are not. This article advises trademark attorneys on how to draft cease and desist letters that may avoid the #trademarkbully label. The following nine elements are common among some of some of the more notable trademark cease and desist letters that are praised by the media as being excessively kind: (1) informal or funny salutations; (2) generous lead time to cease the infringing activity; (3) offers something of value; (4) compliments the target; (5) flexible response date; (6) written in brand voice; (7) no legalese, no citation to caselaw or statutes, and no threat of legal action; (8) no boasting about client's prominence; and (9) no USPTO registration information.

TABLE OF CONTENTS

---

*B.S., Northern Arizona University; M.B.A., Pepperdine University; J.D., University of New Mexico School of Law. Thank you to Professor Nathalie Martin for her encouragement to pursue the #trademarkbully topic, and to Ashley Krause, Kristen Farmer, Adam Scoville, and Jennifer Castro for their inspiration to pursue a career in intellectual property.

INTRODUCTION

A trademark owner must walk a fine line between being too zealous in enforcing its rights and not being zealous enough. The stronger a mark and the more goodwill that attaches to it, the more

> aggressive an owner is expected and entitled to be in asserting its rights against others.[1]

The above quote has some truth to it, but larger trademark owners must be cautious in light of recent trends where smaller businesses defend themselves by appealing to public sentiment and shaming the larger business on social media. This article is written from the perspective of the corporate attorney who represents the larger corporation in a trademark dispute and assumes that the reader has at least a general understanding of trademark rights and some awareness of the "trademark bully" smear tactic being used by *pro se* trademark infringers. This article contains original research in the form of interviews with managers of businesses that have been threatened by large companies for using their trademarks, as well as with an attorney who wrote one of the most successful cease and desist letters in the public domain. In that way, this article brings something completely unique to legal scholarship.

Crying #trademarkbully is one way that small businesses can defend against trademark owners seeking to police the misuse of their trademark rights. The #trademarkbully label on social media can be embarrassing to attorneys and can prevent trademark owners from seeking preliminary enforcement action against infringement targets. In turn, this can prevent trademark owners from policing their trademark rights and can therefore increase the likelihood of trademarks becoming generic.

To date, most scholarly articles on the trademark bullying issue illustrate how shaming trademark owners can be an effective means to defend against trademark infringement. This existing body of work has likely increased the number of small organizations that cry #trademarkbully on social media. While these strategies may be beneficial to smaller organizations, little scholarly work exists to assist trademark owners in mitigating the likelihood that a #trademarkcrier labels them a #trademarkbully on social media.

This article has two interrelated goals: (1) to suggest and compile ways that trademark owners, and their attorneys, can draft cease and desist letters that will avoid the #trademarkbully hashtag on social media; and (2) to present effective means of responding to the #trademarkbully accusation over the phone or email. For illustrative purposes, Part I begins with the story of the TACO TUESDAY® registration mark that demonstrates the transformation of an every-day cease and desist letter into a 2019 fashionable trademark bully smear campaign that made national news.[2] Part II summarizes previous scholarly work regarding the

---

[1] U.S. DEPT. OF COMMERCE, REPORT TO CONGRESS ON TRADEMARK LITIGATION TACTICS AND FEDERAL GOVERNMENT SERVICES TO PROTECT TRADEMARKS AND PREVENT COUNTERFEITING (2011).

[2] *See infra* notes 9–18 and accompanying text.

effectiveness of the #trademarkbully hashtag on social media.[3] Part III explains why cease and desist letters do not need to contain legal statements and also suggests factors that may lead to the #trademarkbully label.[4] Part IV analyzes the section-by-section differences in cease and desist letters labeled #trademarkbully by small businesses and the media vs. cease and desist letters that are praised[5] by small businesses and the media.[6] Part V offers advice on how to respond when an infringer uses the "trademark bully" label over the phone or email.[7]

I. BACKGROUND ON HOW AND WHY TRADEMARK OWNERS ARE LABELED #TRADEMARKBULLY USING THE TACO TUESDAY® EXAMPLE.

A trademark may be cancelled if the trademark owner "does not control, or is not able legitimately to exercise control over, the use of such mark."[8] For example, the TACO TUESDAY® registration mark was awarded to Taco John's Seasonings Limited Partnership ("Taco John's") on December 19, 1989.[9] Taco John's is a Mexican quick-service restaurant brand based in Wyoming that has been in operation since 1969.[10] As of 2019, Taco John's operates and franchises nearly 400 restaurants in 23 states[11] and is listed as the 183rd largest franchise in America, ahead of household name franchise restaurants like Sizzler and Weinerschnitzel.[12]

Taco John's has garnered negative publicity because it was labeled a #trademarkbully on social media as a result of policing its TACO TUESDAY® trademark.[13] A summary of the situation goes like this: Taco John's becomes aware of another company (most likely a restaurant or bar) using the phrase "Taco Tuesday" to promote discounted tacos for sale on Tuesday. Taco John's sends the following cease and desist letter to the infringing company, which appears to be written in a professional tone:

---

3 *See infra* notes 29–35 and accompanying text.

4 *See infra* notes 36–45 and accompanying text.

5 Certain cease and desist letters are effective at avoiding the #trademarkbully label and others are not. Letters that received positive media attention for being excessively kind are referred to as "praised" letters.

6 *See infra* notes 45–70 and accompanying text.

7 *See infra* notes 72–82 and accompanying text.

8 Lanham Trade-Mark Act, 15 U.S.C. § 1064(5) (2016).

9 TACO TUESDAY, Registration No. 1,572,589.

10 TACO JOHN'S, https://tacojohnsfranchise.com (last visited Oct. 21, 2019).

11 TACO JOHN'S, https://tacojohns.com/company/history (last visited Oct. 21, 2019).

12 Franchise Times, Top 200+, THE LARGEST FRANCHISE SYSTEMS BASED IN THE UNITED STATES ACCORDING TO GLOBAL SYSTEMWIDE SALES, https://www.franchisetimes.com/Top200-2019. October 21, 2019 (follow hyperlink).

13 Jenny G. Zhang, *Your Community Taco Tuesday Could Come with a Cease-and-Desist from Taco John's*, EATER (Aug. 14, 2019, 4:40 PM), https://www.eater.com/2019/8/14/20806047/taco-tuesday-taco-johns-trademark-controversy.

> Dear Sir or Madam:
>
> Recently I became aware that Freedom's Edge Brewing Company is using the phrase "Taco Tuesday" to advertise a daily facebook [sic] special.
>
> The purpose of my letter is to let you know that Taco Tuesday® has been a federally registered service mark of our affiliate, Taco John's Seasonings Limited Partnership, since 1989. We certainly appreciate our fellow community member's enthusiasm for tacos on Tuesday and the term is often used inadvertently. However, it is still extremely important to us to protect our rights in this mark because it is a distinctive and important representation of the origin of our products and services and also of the goodwill of our company.[14]

Thereafter, the target takes a picture of only the first half of the cease and desist letter and posts it to their company's social media page.[15] The target then has some disparaging words to say about Taco John's in an effort to persuade sympathetic followers to engage with the post.[16] A media frenzy ensues, the cease and desist letter goes viral, and Taco John's is shamed as a corporate #trademarkbully.[17]

This scenario raises a legal and social conundrum for Taco John's and their franchisees—either stop policing TACO TUESDAY® and run the risk of losing the mark due to it becoming generic, and thus joining the ranks of former brands like Escalator,[18] or send a seemingly professional cease and desist letter and suffer the effects of negative publicity by being shamed on social media. No doubt this is punishment for registering a great trademark. Although the Taco John's attorney likely intended to draft the letter in a professional tone and with good intentions, the letter contains several elements that might have led the target to shame it on social media. Those elements are described below in Section III and IV(C)(2). This also why it is beneficial for attorneys to consider the nine common elements of the Fab Four Letters analyzed below in Section IV.

---

[14] Freedom's Edge Brewing Company (@FreedomsEdgeBrewing), FACEBOOK (July 30, 2019, 12:09 PM), https://www.facebook.com/FreedomsEdgeBrewing/photos/a.541274939292094/2335567686529468.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Haughton Elevator Co. v. Seeberger (Otis Elevator Co. Substituted), 85 U.S.P.Q. 80 (Dec. Comm'r Pat. 1950).

A. Interview with a Manager from Freedom's Edge Brewing Company

During an interview with a manager from Freedom's Edge Brewing Company (one of the small businesses that received the above mentioned Taco John's cease and desist letter),[19] the manager explained the action that prompted their advertisement for "TACO TUESDAY" was a taco truck that sat out in front of the brewery.[20] Freedom's Edge is a small brewery with only a handful of employees and does not sell food,[21] let alone tacos.[22] When the Taco John's letter arrived, the manager observed that the Freedom's Edge employees were intimidated and scared.[23] The employees were worried about being taken to court over something they felt was "silly and trivial."[24] The manager thought that people who work in big businesses are accustomed to receiving letters from attorneys, but the small Freedom's Edge operation is not.[25]

The manager said that Freedom's Edge posted the Taco John's letter on their Facebook page merely in jest.[26] The manager also said that after posting the letter, she and the employees were comforted to see all the support for the brewery and that helped them to feel that the "TACO TUESDAY" mistake was not as big of a deal as they initially thought.[27] The manager also felt that posting the letter was a double edge sword, because some people posted negative comments thinking it was petty for Freedom's Edge to post the letter.[28]

---

[19] Telephone Interview with Anonymous Manager, Freedom's Edge Brewing Company (Oct. 24, 2019). The source's name is kept anonymous for personal reasons.

[20] Mead Gruver, *Taking the Fun Out of 'Taco Tuesday,'* VALLEY NEWS (Aug. 20, 2019, 10:00 PM), https://www.vnews.com/Company-stirs-debate-with-defense-of-Taco-Tuesday-trademark-27863793. ("Taco John's last month sent a warning to a brewery five blocks from its national headquarters for using the term to advertise a taco truck that parks outside its establishment once a week.").

[21] *Id.*

[22] Bill Bostock, *'Taco Tuesday' is Actually Trademarked, and Harshly Policed with Legal Threats from a Taco Chain Based in Wyoming*, BUSINESS INSIDER (Aug. 14, 2019, 5:13 AM), https://www.businessinsider.com/taco-tuesday-trademark-taco-johns-legal-woes-2019-8. ("We have nothing against Taco John's but do find it comical that some person in their corporate office would choose to send a cease and desist to a brewery that doesn't sell or profit from the sales of tacos.").

[23] Telephone Interview with Anonymous Manager, *supra* note 19.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

II. THE PROBLEM: SHAMING A TRADEMARK OWNER CAN BE AN EFFECTIVE MEANS TO DEFEND AGAINST INFRINGEMENT

A. Why Infringing Businesses Cry #Trademarkbully

To understand trademark bullying, one must first understand why an infringing business is more likely to cry #trademarkbully on social media than to respond in a professional manner. Previous scholarly work indicates that small businesses lack the funds to afford legal counsel to respond to cease and desist letters, let alone to litigate.[29] The motivation likely runs much deeper than avoiding litigation expenses. Attorneys who represent large corporations need to understand that for every small business they are opposing, there likely exists an entrepreneur behind the scenes. The entrepreneur may feel that they have risked "everything" to build their business. A standard cease and desist letter typically sent to other attorneys may put the entrepreneur in a perceived position of weakness and vulnerability.

The entrepreneur probably lacks the financial resources to seek legal advice, so they may be placed in reaction mode upon receipt of a cease and desist letter and be forced to strike back. There is no case law that definitively states what is and what is not trademark bullying. However, when at war in a trademark dispute, each side is entitled to use all the ammunition it has.[30] Ammunition may very well include shaming a cease and desist letter on social media.

B. Even if They Could Afford it, Small Businesses Should Not Litigate Trademark Disputes

According to scholar Leah Chan Grinvald, who specializes in trademark law, the structure of trademark law favors large businesses and disfavors small businesses[31] for the following three reasons: (1) there is little precedent in trademark infringement cases for smaller businesses to use because the 'likelihood of confusion' test is considered an issue of fact at the trial level, and trademark infringement cases are typically fact-specific;[32] (2) few statutory defenses are available for small businesses to claim that their use of the mark is appropriate;[33]

---

[29] Leah Chan Grinvald, *Shaming Trademark Bullies*, 2011 WIS. L. REV. 625, 653 [hereinafter *Shaming*].

[30] "[I]nvocation of the minor brands rights is justifiable on the grounds that in going to war for Sure anti-perspirant, P&G was entitled to use all the ammunition it had." Procter & Gamble Co. v. Johnson & Johnson Inc., 485 F. Supp. 1185, 1207 (S.D.N.Y. 1979), *aff'd sub nom*., 636 F.2d 1203 (2d Cir. 1980).

[31] *Shaming*, *supra* note 29, at 657–58.

[32] *Id.* at 658.

[33] *Id.* at 661.

and (3) there are virtually no material consequences for a large business to over-police its trademark rights.[34]

Indeed, small business owners are typically powerless against a trademark infringement claim from a larger trademark owner. The power disparity is likely the triggering event that causes a small business or individual to cry #trademarkbully. Without reasonable options, what else is a small business owner to do except shame the larger business in an attempt to avoid litigation by appealing to public sentiment? It would be rare to find large companies with large legal budgets shaming each other on social media, likely because a personal livelihood is not at stake and the balance of power is equal.

C. Shaming is Effective

Ms. Grinvald also wrote the following excerpt regarding the effectiveness of shaming:

> In September 2009, Hansen Beverage Company [owner of Monster Energy drinks] sent Rock Art Brewery a letter demanding that Rock Art cease and desist its use of "VERMONSTER" as a trademark for beer. The letter stated, in part, "[t]o protect [Hansen's] rights, we must insist that you . . . [i]mmediately cease and desist from any distribution, sale or other use of VERMONSTER in connection with beverages, including the use of any advertising, promotional and point-of-sale materials that include the infringing mark . . . ." Hansen is a multi-million-dollar beverage corporation and Rock Art Brewery is a small brewing company owned by a husband-and-wife team based in Vermont. Hansen's gravamen was that Rock Art's "VERMONSTER" beer allegedly infringed on Hansen's "MONSTER ENERGY" trademarks. Instead of capitulating, Rock Art Brewery fought back, taking to the virtual streets of the Internet and galvanizing public sentiment against Hansen. Rock Art Brewery's YouTube video garnered over fifty thousand viewers within the first couple of days of its posting, and over ten thousand members in the Facebook group, "Vermonters and Craft Beer Drinkers Against Monster." The end result was an amicable settlement agreement that allowed Rock Art to continue its use of "VERMONSTER" as it had before.[35]

---

[34] *Id.*

[35] *Id.* at 627.

Ms. Grinvald's illustration of the Vermonster case shows what most small businesses hope to achieve by crying #trademarkbully.

III. The Perfect Storm for Being Labeled a #Trademarkbully

A. Cease and Desist Letters Do Not Need to Contain Legal Statements

Cease and desist letters do not need to contain legal statements. In fact, cease and desist letters carry little legal weight and are not required to contain a declaration of a trademark owner's rights. Therefore, if the point of the letter is to persuade a small business to stop using a certain mark, then the letter need not contain any legalese… at all. As Ms. Grinvald explains, "[t]here is no reason to use legalese other than as an intimidation tactic, and a cease-and-desist letter can easily convey its seriousness in plain English."[36]

B. Five Factors That Could Lead to Being Labeled #Trademarkbully

Scholar William T. Gallagher, a specialist in trademark law, previously conducted a qualitative empirical study[37] on the use of cease and desist letters to police trademark infringement. Mr. Gallagher's research indicates that the following factors may indicate that a cease and desist letter could be venturing into #trademarkbully territory:

1. The Enforcement Cost is High for Either Side[38]

The cost of enforcement is probably high in every infringement matter. The client is likely being billed for communications leading up to sending the letter, and there may be pressure to end the matter with one letter. However, it may not be worth it. In such a situation, there is the temptation to be overly aggressive, which in turn could lead to the #trademarkbully label. It is equally important to consider the estimated cost to the target when determining if the letter is in #trademarkbully territory. For example, consider a small business with an annual gross revenue of $100,000. If seeking legal advice and responding to the letter costs the small business $1,000, then the small business will have to spend approximately one percent of its annual gross revenue. Many small business owners faced with a similar decision may decide to shame the sender first and seek legal advice second.

---

[36] Leah Chan Grinvald, *Policing the Cease-and-Desist Letter*, 49 U.S.F. L. Rev. 411, 420–21 (2015).

[37] William T. Gallagher, *Trademark and Copyright Enforcement in the Shadow of IP Law*, 28 Santa Clara Computer & High Tech. L.J. 453, 454 (2012).

[38] *Id.* at 475–76.

2. The Alleged Trademark Infringement Involves the Trademark Owner's "Core" Intellectual Property[39]

As Mr. Gallagher states, "enforcement efforts were much more likely to be undertaken against potential targets when the alleged infringement involved the client's 'core' IP, or 'crown jewels[.]'"[40] It therefore appears that if the stakes are higher for the client, the pressure to be overly aggressive may be higher.

3. The Target is a Competitor[41]

Enforcing trademark rights against a competitor is a high priority for most trademark owners.[42] The reasons for the heightened priority include enraging the competitor, avoiding unfair competition, and forcing the competitor to spend money, thereby increasing the competitor's cost of doing business.[43] If the target of the cease and desist letter is a competitor, it will understand the unstated reasons for the letter. The competitor will therefore be placed into reaction mode.

4. The Target is Smaller and Less Sophisticated Than the Trademark Owner[44]

Trademark owners are more likely to target smaller and less sophisticated targets because it is easier and the target is less likely to have the resources to push back.[45] Schoolyard rules apply here: picking on the little guy is more likely to make the client look like a bully. The smaller business can quickly and easily stand up for themselves by posting the letter online and labeling the client a bully. If the target is smaller and less sophisticated than the trademark owner, then the attorney may need to take a step back and consider if they are in #trademarkbully territory.

5. The Target is Active on Social Media

Taking Mr. Gallagher's research one step further, it follows that if the target has a social media presence, then the target at least has an avenue to use social media to its advantage. Professional organizations, such as engineering firms or accounting firms, are less likely to be active on social media than say a brewery, realtor, or author. The difference is that the brewery, realtor, and author are consumer-facing businesses that depend on social media to attract business,

---

39 *Id.* at 476.
40 *Id.*
41 *Id.* at 476–77.
42 *Id.*
43 *Id.* at 477.
44 *Id.* at 478–79.
45 *Id.*

whereas the professional firms are business-to-business organizations with less of a need to interact with consumers. Therefore, if a small business relies on social media for marketing and advertising, then social media attacks are in its wheelhouse.

IV. THE SOLUTION: SECTION-BY-SECTION COMPARISON BETWEEN PRAISED LETTERS AND SHAMED LETTERS[46]

There is no real way to prevent someone from posting a cease and desist letter on social media. In the event that someone does post a letter, efforts should be taken to ensure that there is less of a chance it is accompanied by a caustic hashtag. It would be helpful to consider four trademark cease and desist letters ("Fab Four Letters") sent from large companies to small businesses that are praised as being exceedingly kind. The Fab Four Letters showed up in my research more often than recent letters and appear to me to be classics. Therefore, my research is based on the commonalities present among these four letters. The Fab Four Letters are all applauded by the media and by the small businesses and individuals who received them. Moreover, the Fab Four Letters have another silver lining. They appear to be valuable marketing pieces for the trademark owners.

A. The Fab Four Letters

1. Bud Light

In 2017, Bud Light ran a television commercial marketing campaign that featured people in medieval times sitting at a large formal dinner offering Bud Light to the king as a gift.[47] Upon receipt of the Bud Light, the king would say from the throne, "you are a true friend of the crown, Dilly Dilly" and hold up the Bud Light beer bottle to salute the gift bearer.[48] The crowd would then all hold up their Bud Light beer bottles and say "Dilly Dilly" in unison.[49] Someone then approached the king and offered a bottle of wine as a gift and the king was displeased.[50] The king said to the man offering wine, "please follow Sir Brad, he's going to give you a private tour of the pit of misery."[51] Other Bud Light commercials in the same

---

[46] Letters that were posted on social media with the intention of shaming the trademark owner are referred to as "shamed" letters. "Shaming" refers the use of social media to attack an attorney or organization by posting the attorney's cease and desist letter online. The purpose of the attack is to embarrass the attorney or organization, as retribution for the attorney's initial letter.

[47] Bud Light Commercial, *Bud Light TV Commercial, 'Banquet'*, ISPOT.TV, https://www.ispot.tv/ad/wTA8/bud-light-banquet [hereinafter *Banquet*].

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

campaign offered viewers the chance to win Super Bowl tickets for life.[52] Anheuser-Busch, LLC previously registered the tagline, "Dilly Dilly."[53]

Later in 2017, Bud Light caught wind of a brewery in Minneapolis marketing a beer called "Dilly Dilly Mosaic Double IPA." Instead of sending a cease and desist letter, Bud Light sent an actor dressed as a town crier from medieval times to read a hilarious script to the brewery that asked the brewery to discontinue marketing Dilly Dilly Mosaic Double IPA. The actor dressed, spoke, and acted exactly like the characters in the above mentioned "Dilly Dilly" TV campaign. The effect of the statement is best understood by watching the video,[54] but this is what the actor read aloud in what appears to be the lobby of Modist Brewing Company:

> Dear friend of the Crown, Modist Brewing Company. Congratulations on the launch of your new beer, Dilly Dilly Mosaic Double IPA! Let it be known that we believe any beer shared between friends is a fine beer indeed. And we are duly flattered by your loyal tribute. However, "Dilly Dilly" is the motto of our realm, so we humbly ask that you keep this to a limited-edition, one-time-only run. This is by order of the king. Disobedience shall be met with additional scrolls, then a formal warning, and finally, a private tour of the pit of misery. Please send a raven, letter or electronic mail to let us know that you agree to this request. Also, we will be in your fair citadel of Minneapolis for the Super Bowl, and would love to offer two thrones to said game for two of your finest employees to watch the festivities and enjoy a few Bud Lights. On us. Yours truthfully, Bud Light.[55]

Bud Light's letter was met with positive fanfare and made national news as being a praised cease and desist letter.[56] Bud Light's letter was praised because it did not put the owners or employees of Modist Brewing Company into a perceived position of weakness and vulnerability. Note that Bud Light's letter is informal, does not demand that Modist immediately cease its infringing activity, compliments Modist's success, offers something of value to Modist in the form of Super Bowl tickets, and does not use legalese.

---

[52] Bud Light Commercial, *Bud Light Super Bowl Tickets for Life Sweepstakes TV Commercial, 'Handouts'*, ISPOT.TV, https://www.ispot.tv/ad/wuFy/bud-light-super-bowl-tickets-for-life-sweepstakes-generous-king.

[53] DILLY DILLY, Registration No. 5,450,256.

[54] *Banquet*, *supra* note 47.

[55] Joe Patrice, *Bud Light Lawyers Send Town Crier to Deliver Cease and Desist Letter*, ABOVE THE LAW (Dec. 4, 2017, 12:51 PM), https://abovethelaw.com/2017/12/bud-light-lawyers-send-town-crier-to-deliver-cease-and-desist-letter.

[56] *Id.*

2. Netflix

In 2017, Netflix sent a cease and desist letter to protect its trademark rights regarding the hit series Stranger Things. Netflix wrote the letter entirely in the *Stranger Things* brand voice. Anyone who has seen the show would agree that the language appears to have been written by one of the child characters featured in the show. The media loved this cease and desist letter and many articles were written that praised Netflix's sense of humor.[57] Here is the letter in its entirety:

> Dear [target's first name],
>
> My walkie talkie is busted so I had to write this note instead. I heard you launched a Stranger Things pop-up bar at your Logan Square location. Look, I don't want you to think I'm a total wastoid, and I love how much you guys love the show. (Just wait until you see Season 2!) But unless I'm living in the Upside-Down, I don't think we did a deal with you for this pop-up. You're obviously creative types, so I'm sure you can appreciate that it's important to us to have a say in how our fans encounter the worlds we build.
>
> We're not going to go full Dr. Brenner on you, but we ask that you please (1) not extent the pop-up beyond its 6 week run ending in September, and (2) reach out to us for permission if you plan to do something like this again. Let me know as soon as possible that you agree to these requests.
>
> We love our fans more than anything, but you should know that the demogorgon is not always as forgiving. So please don't make us call your mom.
>
> Thanks,
> [Signature][58]

Netflix's letter was praised because it does not put the infringing small business into a perceived position of weakness or vulnerability. Similar to Bud Light's letter, Netflix's letter is funny, informal, addresses the target by first name, does not use legalese, and does not demand that the target immediately cease its infringing activity. However, rather than offering something of additional value, Netflix allowed the target to continue their campaign through the end of their

---

[57] Tim Nudd, *Netflix Sent the Best Cease-and-Desist Letter to This Unauthorized Stranger Things Bar*, ADWEEK (Sep. 20, 2017, 5:13 AM), https://www.adweek.com/creativity/netflix-sent-the-best-cease-and-desist-letter-to-this-unauthorized-stranger-things-bar/.

[58] *Id.*

planned six-week run date. Netflix's tactic did not have the effect of scaring the target and the letter turned a negative situation into a positive marketing piece for both companies.

3. TGI Fridays

In 2017, the media praised the following TGI Fridays cease and desist letter that asked a Chicago bar to not dress up as TGI Fridays for Halloween:

> Dear [target's first name]:
>
> As the trademark counsel at TGI Fridays, I wanted to reach out regarding Moneygun's plan to dress up as TGI Fridays for Halloween.
>
> It's certainly a rite of passage to dress up as your personal hero for Halloween. After all – TGI Fridays is renowned for being the country's first singles bar and has been credited for creating loaded potato skins and popularizing the Long Island Iced Tea. (You're welcome, by the way.)
>
> Fortunately, we have a number of things you can take off our hands to party like it's always Friday. Please see enclosed gift.
>
> All is yours to keep…we don't need it anymore.
>
> UNfortunately (for you – not us), trademark law requires us to protect our brands and to take action against any use that might cause confusion or diminish the value of our trademarks. I'm concerned that your event – featuring "TGI" branding, our logo, a variation of our IN HERE, IT'S ALWAYS FRIDAY slogan, and so on – would cross that line.
>
> As such, we must ask that you avoid using TGI Fridays' trademarks, logos, and other property in your event.
>
> Seriously. Don't. Thanks. Happy Halloween.[59]

---

[59] Ashok Selvam, *TGI Fridays Won't Sue MONEYGUN Over Pop-Up, Sends Them Flair*, EATER CHICAGO (Oct. 27, 2017, 1:07 PM), https://chicago.eater.com/2017/10/27/16560494/tgifridays-chicago-pop-up-halloween-moneygun-west-loop-cease-desist-letter.

The media and the target praised[60] the TGI Fridays letter. The letter is informal and addresses the target as if they are a friend. The most striking informal element of the TGI Fridays letter is that it closes with "Seriously. Don't. Thanks. Happy Halloween." The letter does not allow the target to continue with the Halloween costume plan, but the letter was sent one week prior to Halloween, so the small business could still have time to plan a different costume for the bar. TGI Fridays' letter and Netflix's letter are similar in that they both allow the target plenty of time to cease the infringing activity. Next, TGI Fridays' letter is funny and offers a gift of flair to the bar.[61] The letter goes on to state TGI Fridays' position without using legalese and does not boast about the prominence of the TGI Fridays brand. The combination of these elements appears to give the letter a praiseworthy status that turned into a positive public relations piece for TGI Fridays.

4. Jack Daniel's

The final Fab Four Letter is regarded as the "world's nicest cease and desist letter ever."[62] The letter is not humorous like the previous letters, but it contains many of the same elements as the Bud Light, Netflix, and TGI Fridays letters.

> Dear [target's last name]:
>
> I am an attorney at Jack Daniel's Properties, Inc. ("JDPI") in California. JDPI is the owner of the JACK DANIEL'S trademarks (the "Marks") which have been used extensively for many years in connection with our well-known Tennessee whisky product and a wide variety of consumer merchandise.
>
> It has recently come to our attention that the cover of your book *Broken Piano for President*, bears a design that closely mimics the style and distinctive elements of the JACK DANIEL'S trademarks. An image of the cover is set forth below for ease of reference.
>
> We are certainly flattered by your affection for the brand, but while we can appreciate the pop culture appeal of Jack Daniel's, we also have to be diligent to ensure that the Jack Daniel's trademarks are used correctly. Given the brand's popularity, it will probably come

---

60 *Id.*

61 *Id.* "Flair" refers to the small items Fridays employees wear on their uniforms such as buttons. The term "flair" was popularized in Mike Judge's 1999 film Office Space.

62 Avi Dan, *The World's Nicest Cease-and-Desist Letter Ever Goes Viral, Sells Books*, FORBES (Jul. 26, 2012, 12:38 AM), https://www.forbes.com/sites/avidan/2012/07/26/the-worlds-nicest-cease-and-desist-letter-ever-goes-viral-sells-books/#394233e86c11.

> as no surprise that we come across designs like this on a regular basis. What may not be so apparent, however, is that if we allow uses like this one, we run the very real risk that our trademark will be weakened. As a fan of the brand, I'm sure that is not something you intended or would want to see happen.
>
> As an author, you can certainly understand our position and the need to contact you. You may even have run into similar problems with your own intellectual property.
>
> In order to resolve this matter, because you are both a Louisville "neighbor" and a fan of the brand, we simply request that you change the cover design when the book is re-printed. If you would be willing to change the design sooner than that (including on the digital version), we would be willing to contribute a reasonable amount towards the costs of doing so. By taking this step, you will help us to ensure that the Jack Daniel's brand will mean as much to future generations as it does today.
>
> We wish you continued success with your writing and we look forward to hearing from you at your earliest convenience. A response by [eleven days after the letter was sent] would be appreciated, if possible. In the meantime, if you have any questions or concerns, please do not hesitate to contact me.[63]

The Jack Daniel's letter also shares a few elements with the Bud Light, Netflix, and TGI Fridays letters. First, the letter is somewhat informal and very polite. The attorney does not use overly technical legalese and does not illustrate the prominence of the Jack Daniel's brand. The attorney does not demand that the target immediately cease the infringing activity, but instead allows the author to sell through his existing inventory. Then, the attorney offers something of value to the target by offering to pay for part of the cost to reprint the books if the author wishes to replace the inventory now. The combination of praised elements in the Jack Daniel's letter likely helped the target to maintain his perceived perception of power and therefore, not shame Jack Daniel's as a trademark bully.

B. Analysis of the Nine Common Elements Among the Fab Four Letters

The Fab Four Letters contain the following nine elements:

---

63 *Id.*

1. Informal or Funny Salutations

The openings and closings are typically informal, humorous, and contain soft statements. Some of the Fab Four Letters also address the target by first name. This is important because the target is more likely to be put at ease and read the letter with a positive frame of mind.

2. Generous Lead Time to Cease Infringing Activity

There is no directive to immediately cease the alleged infringement. Instead, the attorney politely requests that the target discontinue the activity past the pre-determined run date already established. It follows that a small business owner is less likely to feel threatened when there is no threat of a financial penalty or future legal action from the opposing attorney.

Consider a small business owner who unintentionally creates a building sign that infringes on a client's trademark. In order to take down the building sign, the small business owner will need to spend a few thousand dollars and hire a third-party company to perform the removal. It takes time for the small business owner to both reallocate the required capital and wait in queue for the third-party sign company to remove the sign. Placing a stringent deadline for removal may put the small business owner in a position of perceived weakness and increase the likelihood that it will then become #trademarkbully time.

Instead, trademark owners should consider working with the small business owner to find a more appropriate time for them to cease their infringing activity. In the building sign hypothetical, maybe the building is due for renovation in a few months and the target would have to take the sign down anyway. The point is to avoid stringent temporal demands when possible.

3. Offers Something of Value

In most of the Fab Four Letters, the attorney typically offers something of value to the target. Bud Light offered Super Bowl tickets, TGI Fridays offered flair, and Jack Daniel's offered to cover some of the expense of reprinting. It may sound odd to offer a gift to an infringing business, but the gesture alone can pay itself back as a positive marketing piece.

While it is not always feasible for a trademark owner to offer something of value to an infringing business, consider other corporate assets at the client's disposal. For example, if the target is using infringing design elements in their advertising, would it be possible to offer that the client's in-house marketing department create new design elements for the target? In this scenario, the trademark owner is not incurring a direct expense and the target may not take the client up on the offer anyway. It is likely the gesture alone that will ensure the target

remains in a perceived position of power, which will reduce the chances the trademark owner is labeled a #trademarkbully.

4. Compliments the Target

There is no better way to defuse a situation than to issue a genuine compliment. The Fab Four Letters did this by congratulating the target on their success or thanking them for being a fan of the trademark owner's brand.

5. Flexible Response Date

The Fab Four letters do not demand that the target respond by a certain date. The Bud Light and Netflix letters do not provide a response date, the TGI Fridays letter does not ask for a response at all, and the Jack Daniel's letter gives an eleven-day lead time for a response, but contains the language, "[a] response by [date] would be appreciated, if possible." Therefore, it appears that it is best to employ a flexible response date in order to stay off the #trademarkbully radar. Giving the target a flexible response date alleviates much of the stress associated with a stringent temporal demand. The target will likely feel more at ease and may be less likely to post the letter online.

6. Written in Brand Voice

The Fab Four Letters are written in the brand's voice. The letters almost seem to be written by the trademark owner's marketing department with the intention that the letter will be posted on social media. If possible for the brand, the trademark owner's marketing department should review the letter to safeguard that the letter reflects positively on the brand's image.

7. No Legalese, no Citation to Caselaw or Statutes, and no Threat of Legal Action

The Fab Four Letters do not use legalese, do not cite to caselaw or statutes, and do not threaten legal action. A target might be confused by legalese, might be scared by citations to caselaw or statutes, and will likely take a defensive position to threats of legal action. The scared and confused targets are the ones who have a greater propensity to cry bully.

8. No Boasting About the Client's Prominence

The Fab Four Letters do not state the size of the trademark owner's company nor do they highlight the prominence of the trademark. Statements of prominence are, however, present in the shamed letters discussed below.

Statements of prominence may have a negative effect if they are used to bolster the size of the client. The target will likely already know who the trademark owner is and can Google further information. There is no need to further state that the client is bigger and has a superior bargaining position. Such a statement can have an intimidation effect and lead the target to feel as if they are being bullied by a larger company.

9. No USPTO Registration Information

Providing USPTO registration information is reasonable when communicating with other attorneys, but there is no need to use this tactic when communicating with a small business owner. None of the Fab Four Letters use the USPTO registration tactic. Omitting registration information makes sense because registration information may frighten the small business owner into believing that legal action is imminent. Enclosing USPTO registration information is also unnecessary and does not give a cease and desist letter greater legal weight.

To summarize this section, when the perfect storm is present as discussed in Section III, think of the cease and desist letter as a marketing piece that will be published on the front page of tomorrow's newspaper. If written properly, the cease and desist letter can act as a valuable marketing piece for the trademark owner and add value to the brand. A properly written letter will protect the brand reputation from the harms of being labeled a #trademarkbully.

C. #Trademarkbully: The Shamed Letters

1. Louis Vuitton

The case of Louis Vuitton and the University of Pennsylvania is an example of what is viewed as trademark bullying. In 2012, Louis Vuitton sent a letter to the dean of the University of Pennsylvania Law School asking the school to stop using elements of a trademark registered by Louis Vuitton in a poster that advertised "IP issues in fashion law:"[64]

> I am the Director of Civil Enforcement, North America, for Louis Vuitton Malletier ("Louis Vuitton"). I write to express our concerns over the unauthorized use of our trademarks to promote the March 20, 2012 Penn Intellectual Property Group event, "IP Issues in Fashion Law."

---

[64] Staci Zaretsky, *A Top Law School Tells a High-End Fashion House Where to Stick Its Cease and Desist Letter*, ABOVE THE LAW (Mar. 5, 2012, 2:05 PM), https://abovethelaw.com/2012/03/a-top-law-school-tells-a-high-end-fashion-house-where-to-stick-its-cease-and-desist-letter/; see also Letter from Michael Pantalony, Dir. of Civil Enf't, N. Am., Louis Vuitton Malletier, to Michael A. Fitts, Dean of University of Pa. Law Sch. (February 29, 2012) (on file with author).

Louis Vuitton is the owner of world famous registered and common law trademarks, including the following trademarks as shown below (the "LV Trademarks"):

[Images]

[Paragraph regarding the history of the trademark.]

[Paragraph regarding the prominence of the Louis Vuitton brand.]

While every day Louis Vuitton knowingly faces the stark reality of battling and interdicting the proliferation of infringements of the LV Trademarks, I was dismayed to learn that the University of Pennsylvania Law School's Penn Intellectual Property Group had misappropriated and modified the LV Trademarks and Toile Monogram as the background for its invitation and poster for the March 20, 2012 Annual Symposium on "IP Issues in Fashion Law." A copy of the invitation/poster is attached as Exhibit A.

This egregious action is not only a serious willful infringement and knowingly dilutes the LV Trademarks, but also may mislead others into thinking that this type of unlawful activity is somehow "legal" or constitutes "fair use" because the Penn Intellectual Property Group is sponsoring a seminar on fashion law and "must be experts." People seeing the invitation/poster may believe that Louis Vuitton either sponsored the seminar or was otherwise involved, and approved the misuse of its trademarks in this manner. I would have thought the Penn Intellectual Property Group, and its faculty advisors, would understand the basics of intellectual property law and know better than to infringe and dilute the famous trademarks of fashion brands, including the LV Trademarks, for a symposium on fashion law. (Louis Vuitton believes that education of the public about intellectual property issues is important and has sponsored such activities in the past. In fact, Louis Vuitton is a corporate sponsor of Fordham Law School's Fashion Law Institute).

Louis Vuitton is proud of its reputation for protecting intellectual property and creativity. We hope, and expect now that this action has been brought to your attention, that immediate steps will be taken to stop all use of this invitation/poster that violates the LV Trademarks. Please contact me within five days to assure me that

> steps have been taken to avoid confusion and dilution of the LV Trademarks. Your understanding and anticipated cooperation is appreciated.[65]

The Louis Vuitton letter contains several elements that differ from the Fab Four Letters including a formal and combative introduction, paragraphs that boast about Louis Vuitton's prominence, and statements that put the target in a perceived position of weakness. The letter appears combative because it uses phrases such as, "I am the Director of Civil Enforcement," "I was dismayed to learn," and "[t]his egregious action."[66] The letter then uses two paragraphs to boast about the history and prominence of Louis Vuitton's trademarks. The letter further puts the target in a perceived position of weakness by threatening legal action, demanding that the alleged infringement cease immediately, and requiring an inflexible response date. Combine those elements with the fact that the university setting is mostly younger students who are active on social media, there is a greater propensity to label an organization as a #trademarkbully.

Consider how this outcome may have been different if Louis Vuitton followed the nine common elements of the Fab Four Letters. To offer something of value, Louis Vuitton could have sent a free handbag with a suggestion that the handbag be raffled off at the University of Pennsylvania event in order to further promote the event. Louis Vuitton could have written off the expense of the handbag as a marketing sample, foregone the litigation expense, and possibly furthered its brand image (if, of course, such a gesture falls within Louis Vuitton's brand image).

2. Taco John's

The Taco John's letter is included again to highlight the elements that make this letter a risk for trademark bully shaming.[67] The target posted only the first half of the letter, so it is unknown what the second half said.

> Dear Sir or Madam:
>
> Recently I became aware that Freedom's Edge Brewing Company is using the phrase "Taco Tuesday" to advertise a daily facebook [sic] special.
>
> The purpose of my letter is to let you know that Taco Tuesday® has been a federally registered service mark of our affiliate, Taco

---

65 *Id.*
66 *Id.*
67 Zhang, *supra* note 13.

> John's Seasonings Limited Partnership, since 1989. We certainly appreciate our fellow community member's enthusiasm for tacos on Tuesday and the term is often used inadvertently. However, it is still extremely important to us to protect our rights in this mark because it is a distinctive and important representation of the origin of our products and services and also of the goodwill of our company.[68]

Contrast the Taco John's salutation of "Dear Sir or Madam" with the friendlier salutation of the Fab Four Letters that begin with the target's first name. Taco John's, unfortunately, did not address the letter to an individual person.[69] The Taco John's letter then goes on to bolster the prominence of the TACO TUESDAY® mark.[70] Although it is unknown what the rest of the letter said, the first two elements were at least enough to garner public sentiment against Taco John's. The fact that "Taco Tuesday is so well known ensured the letter go viral as a shamed letter.[71]

V. HOW TO RESPOND WHEN TARGETS USE THE "TRADEMARK BULLY" LABEL OVER THE PHONE OR EMAIL

A. Interview with the Attorney Who Wrote the Jack Daniel's Letter, AKA "The World's Nicest Cease and Desist Letter Ever"

The following points come from an interview with Christy Susman,[72] one of the in-house attorneys who worked on the Jack Daniel's letter. At the time, the letter was praised by the media as the "world's nicest cease and desist letter ever."[73] To preemptively avoid the #trademarkbully label, Ms. Susman indicated there are two factors that may be most important: (1) knowing the audience and (2) staying true to the brand being protected.[74] The legal team's goal should be to ensure that the target does not have the #trademarkbully response, and if the target does have

---

68 FACEBOOK, *supra* note 14.

69 *Id.*

70 *Id.*

71 Gruver, *supra* note 20; Bostock, *supra* note 22.

72 E-mail from Christy Susman, to Paul Martello (Nov. 12, 2019, 2:18 PM MST) (on file with author). Christy Susman was interviewed over seven years after the Jack Daniel's letter went viral. Ms. Susman stated that drafting the letter was a team effort. Brown-Forman, the company that owns the Jack Daniel's brand, was a very collaborative workplace with many employees who took an ownership stake in protecting the Jack Daniel's brand. Working together, the legal department and the Jack Daniel's brand team crafted an approach for handling the matter that was entirely authentic to the brand and its "voice."

73 Dan, *supra* note 62.

74 *See* E-mail from Christy Susman to Paul Martello, *supra* note 72.

the #trademarkbully response, that the legal team can stand behind the letter's tone and contents if it were posted online.[75]

If the target responds negatively, either the attorney or someone from the brand team can call the target to explain the trademark owner's position.[76] The explanation can include why the attorney needed to write the target, why the attorney needs the target's help in complying, and ask for the target's help in protecting the trademark owner's brand.[77] No two situations are alike, and the situation can be better defused if the target believes that the company wants to hear the target's story and work with the target.[78] There is no need to over-lawyer the situation, and an informal conversation is probably best.[79]

Sometimes, paralegals may take the brunt of a target's anger. Paralegals can be instructed to first apologize, explain, and provide context regarding how the goal of the letter was to avoid making the target feel that they were bullied.[80] Next, it may be best for paralegals to pass the target to someone higher up the chain.[81] Depending on the situation, listening to the target to understand the target's side of the story is what is really needed.[82]

CONCLUSION

Crying #trademarkbully on social media is an effective tactic that small businesses can use to defend themselves against trademark owners seeking to police the misuse of their trademark rights.[83] The #trademarkbully label typically occurs when the recipient of an overly aggressive cease and desist letter posts the letter to social media with the intention of shaming the trademark owner. The following five factors may indicate that a cease and desist letter could be venturing into #trademarkbully territory: (1) the enforcement cost is high for either side,[84] (2) the alleged infringement involves the trademark owner's "core" intellectual property,[85] (3) the target is a competitor,[86] (4) the target is smaller and less sophisticated than the trademark owner,[87] and (5) the target is active on social media.

---

75 *Id.*
76 *Id.*
77 *Id.*
78 *Id.*
79 *Id.*
80 *Id.*
81 *Id.*
82 *Id.*
83 *Shaming*, *supra* note 29, at 627.
84 Gallagher, *supra* note 37, at 475.
85 *Id.* at 476.
86 *Id*. at 476–77.
87 *Id.* at 478–79.

Four cease and desist letters sent from large companies to small businesses successfully avoided the #trademarkbully label and have been praised by the media as being exceedingly kind.[88] These four letters contain the following nine elements: (1) informal or funny salutations; (2) generous lead time to cease the infringing activity; (3) offers something of value; (4) compliments the target; (5) flexible response date; (6) written in brand voice; (7) no legalese, no citation to caselaw or statutes, and no threat of legal action; (8) no boasting about client's prominence; and (9) no USPTO registration information. Given this information, it is clear that trademark owners should take these steps to avoid being labeled a #trademarkbully.

---

[88] Patrice, *supra* note 55; Nudd, *supra* note 57; Selvam, *supra* note 59; Dan, *supra* note 62.