Journal of International Business and Law

Volume 19 | Issue 2 Article 6

3-1-2020

The Big Box versus the Mom & Pop Shop: The Beauty of the (Data Privacy) Bills Are in the Eye of the Beholder

Alexander R. Migliorini
Maurice A. Deane School of Law at Hofstra University

THE BIG BOX VERSUS THE MOM & POP SHOP: THE BEAUTY OF THE (DATA PRIVACY) BILLS ARE IN THE EYE OF THE BEHOLDER

Alexander R. Migliorini[*]

I. INTRODUCTION

Some fear that robots may be taking over.[1] Others fear that their Alexa device is listening and recording everything they say, which will later be used against them in some adverse way.[2] While fears of big brother certainly are not new, as illustrated in the fabled but dreaded high school reading requirement, George Orwell's 1984, they are becoming increasingly plausible and less of a farfetched dystopian reality.[3] Public discovery of Cambridge Analytica's use of data as a "psychological warfare tool" sparked a great privacy awakening to the consequences of mass data manipulation capable of interfering with the US democratic process.[4] Although big data is allegedly aimed towards improvement of the consumer experience, people are rightfully reluctant to allow big business to play big brother with their information.[5]

As the world progresses into the digital age, more robust data privacy laws are undoubtedly needed.[6] Consumers have become overwhelmed, due in part to their lack of bargaining power, when dealing with data privacy risks and concerns, such as corporate giants

---

[*] This Note is dedicated to [let me think about this one].

[1] *See* Olivia Solon, *More than 70% of US fears robots taking over our lives, survey finds,* GUARDIAN (Oct. 4, 2017 1:15 EDT), https://www.theguardian.com/technology/2017/oct/04/robots-artificial-intelligence-machines-us-survey.

[2] *See* Kieren McCarthy, *You know that silly fear about Alexa recording everything and leaking it online? It just happened,* REGISTER (May 24, 2018, 6:49 PM), https://www.theregister.co.uk/2018/05/24/alexa_recording_couple/ (reporting a story where a "couple received a phone call from one of the husband's employees . . . telling them she had just received a recording of them talking privately in their home" from their Amazon Alexa device).

[3] *See* Jermelle Macleod, *'1984' is quickly becoming our reality,* DAILY AZTEC (Apr. 17, 2019), https://thedailyaztec.com/94304/opinion/1984-is-quickly-becoming-our-reality/.

[4] *See* Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening,* WIRED (Mar. 17, 2019), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/.

[5] *See* Daniel Newman, *Improving Customer Experience Through Consumer Data,* FORBES (Apr. 4, 2017), https://www.forbes.com/sites/danielnewman/2017/04/04/improving-customer-experience-through-customer-data/#ce454744e64d; *see also* Herb Weisbaum, *Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal,* MSNBC (Apr. 18, 2018, 3:08 PM), https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011.

[6] *See generally Data Security Laws: Private Sector,* NAT'L CONFERENCE OF STATE LEGISLATURES (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx (showing that most states have adopted some form of data privacy protection); *see also Data Protection Laws of the World,* DLA PIPER (last visited Sept. 22, 2019), https://www.dlapiperdataprotection.com/.

buying, selling, and storing personal information.[7] At the same time, some consumers choose to monetize their personal data.[8] With big data becoming increasingly structural to the modern computing systems that underlie many global societies, and with black hat criminals hacking and exploiting data warehouses, the inevitability of government regulation was prominent.[9] The public needed a defender and device to confidently ensure that their personal information remain secure.[10]

Recently, the EU's General Data Privacy Regulation (the "GDPR") has expanded the rights of consumers in relation to their personal information, employing stringent data privacy and security regulations on companies doing business in European nations.[11]This has now become the status quo in the European Union ("EU"); all companies, including small businesses, doing business in the EU must comply to avoid facing harsh penalties.[12] Although companies have sprung up offering assistance with GDPR compliance, smaller businesses nonetheless have become victims of the new regulations due to a lack of international counsel or a GDPR department, thereby giving big corporations a competitive advantage.[13]

More obviously, companies like Facebook, Walmart, and Amazon have no option but to be GDPR compliant, with in-house departments exclusively dedicated to GDPR compliance.[14] However, refocus is drawn on small businesses with operations in, or in possession of, data originating from the EU but that may not be large enough to justify the cost of GDPR compliance.[15] GDPR compliance costs can quickly begin to outweigh the benefits of

---

[7] *See Data Privacy: What the Consumer Really* Thinks, DMA GRP. 4 (Feb. 2018), https://marketing.acxiom.com/rs/982-LRE-196/images/Data%20Privacy%20-%20What%20the%20consumer%20really%20thinks%20FINAL_2018.PDF.

[8] *See, e.g.,* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html; *see also* Stacey-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COL. L. REV. 1369 (2017).

[9] *See generally* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) (intimating a growing concern for data privacy regulation); *see also* iimbobo2779, *Is GDPR going to affect us?*, BLACK HAT WORLD (Apr. 13, 2018), https://www.blackhatworld.com/seo/is-gdpr-going-to-affect-us.1022262/ (explaining on a blog to other "black hatters" how they will be affected by the GDPR).

[10] *See* Andrew Rossow, *The Birth Of GDPR: What Is It and What You Need to Know*, FORBES (May 25, 2018, 7:32 AM), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/; *see generally* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (outlining the objectives showing its intended goal).

[11] Commission Regulation 2016/679, *supra* note 10.

[12] *See id.*; *see also* Thomas Codevilla, *GDPR Compliance Tips for Small and Medium-Sized Businesses*, 47 COLO. LAWYER 12 (2018).

[13] *See Small Businesses Are Buying into Search Engine Optimization---But with Less Than Optimal Effect*, 34 LAWYER'S PC 10 (2017) [*hereinafter* Buying into Search Engine Optimization]; *see also* Codevilla, *supra* note 12; *see also* Henry Kenyon, *GDPR likely to catch many small UK businesses by surprise, survey says,* CQ ROLL CALL (Feb. 1, 2018); *see also* Mark Scott, Laruens Cerulus, & Laura Kayali, *Six months in, Europe's privacy revolution favors Google, Facebook*, POLITICO (Nov. 23, 2018, 2:45 PM), https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/ (last updated Apr. 19, 2019).

[14] *See* Craig McAllister, *What About Small Businesses? The GDPR and its Consequences for Small, U.S.-Based Companies*, 12 BROOK. J. CORP. FIN. & COM. L. 187 (2017).

[15] *See id.*

conducting business abroad, and, therefore, many small and medium-sized companies actively sidestep the GDPR and end up losing out on potential business opportunities.[16]

While the GDPR has certainly sparked global influence and shaped the laws of other countries, some of the states within the United States have adopted and instituted aspects of the GDPR.[17] California has approached its promulgation of data privacy laws with less influence from the GDPR, while New York has taken an approach more closely mirroring the stringent and broadly scoped nature of the GDPR.[18]

This Note shall first discuss the evolution of data privacy throughout the world, then parse the key provisions and cardinal takeaways of the GDPR. Given the highly influential power of the GDPR, this Note will continue by comparing the inevitable and anticipated US response and the regulatory inadequacies and inconsistencies between these different approaches, specifically examining the minimum threshold requirement, the beneficiary of the noncompliance, and the extension of coverage to employee data. Next, for the sake of uniformity, consistency, ease of widespread acceptance, it is urged that the US, with the help of the Uniform Law Commission and other insightful scholars and professionals, draft a Model Data Privacy Act that, at a minimum, addresses the inconsistencies highlighted in this Note. Lastly, although the GDPR's approach may be fitting to European culture, a model act geared toward the US should reflect and conform to the American consumer culture and its values.

II. BACKGROUND

A. History of Data Privacy Laws

Data privacy laws date back as early as and have roots from the US colonial era when eavesdropping was deemed unlawful, defined as "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[19] One of the first laws directly dealing with data privacy emerged in 1776 when the Riksdag passed the Access to Public Records Act.[20] Later, in 1890, American attorneys Samuel D. Warren and Louis Brandeis wrote an article entitled *The Right to Privacy*, which first articulated a formal definition of privacy with the idea of the "right to be left

---

[16] *See* Jonas De Oliveira, *How Much Does GDPR Compliance Cost?*, SEC. METRICS, https://www.securitymetrics.com/blog/how-much-does-gdpr-compliance-cost (last visited Sept. 24, 2019).

[17] *See* Bryan Pistorius, *Breaking Down GDPR and its Influence on U.S. Entities and U.S. Privacy Laws*, MICH. BUS. ENTREPRENEURIAL L. REV. (Mar. 17, 2019), http://mbelr.org/breaking-down-gdpr-and-its-influence-on-u-s-entities-and-u-s-privacy-laws/; *see also* Jessica Davies, *The Impact of GDPR, in 5 Charts*, DIGIDAY (Aug. 24, 2018), https://digiday.com/media/impact-gdpr-5-charts/.

[18] *See id.*

[19] Daniel J. Solove, *Proskauer on Privacy: A Brief History of Information Privacy* Law, PLI (2016), https://ssrn.com/abstract=914271.

[20] *See* Wayne Madsen, HANDBOOK OF PERSONAL DATA PROTECTION 24 (1992) (explaining that the Access to Public Records Act was the first law dealing with data privacy that privileged the public with access to public information); *see also Sveriges Riksdag*, LIBRARY OF CONG., https://www.loc.gov/item/lcwa00095713/ (last updated Jan. 15, 2016) (explaining that the Riksdag is Sweden's supreme decision making an assembly that creates laws, determines taxes and the budget for the central government, and examines the work of the central government).

alone."[21] Approximately sixty years later at the end of 1948, this same concept of a right to privacy was first recognized globally as the twelfth fundamental right in the United Nations' Universal Declaration of Human Rights.[22]

Modern data privacy concerns, however, began to emerge into the limelight with the advent of the Internet in Sweden's 1973 Data Act, which imposed license requirements on information systems that processed personal data.[23] Gaining global traction, the Organization for Economic Cooperation and Development released guidelines in 1980 for the protection of data, resulting from the rise of the use of technology in business dealings. In 1981, the Council of Europe codified the right to privacy in the Data Protection Convention as a legal imperative.[24]

Then, in 1995, the European Commission introduced the EU's Data Protection Directive, the young predecessor to the GDPR, seeking to protect the processing of the sensitive data and consent of individuals.[25] Approximately 14 years later, followed by a few other international efforts along the way, the EU legislature sought reformation, ultimately resulting in the promulgation of the GDPR.[26] While the GDPR is a surfacing buzzword circulating at networking events and grabbing other scholarly and professional attention, new international successor laws and regulations are burgeoning the data privacy laws of the future.[27]

The General Data Protection Regulation 2016/679, more commonly referred to as the GDPR, seeks to regulate the trade of consumer data, primarily targeting companies doing business within the EU and the European Economic Area ("EAA") or transferring data outside the EU or EAA.[28] The emergence of the GDPR sparked global attention barreling beyond the EU as to the expansion of individuals' rights to their data and how businesses control it.[29] The GDPR has undoubtedly changed the landscape of data privacy laws globally, with influence reaching to the US.[30]

However, seldom do laws have absolute portability across borders.[31] Most US member states have adopted some state-statutory standard confronting data privacy.[32] A handful have promulgated, or are in the process of enacting, comprehensive approaches to data

---

[21] *See* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also A Brief History of Data Protection: How Did it All Start?*, EUROCLOUD (Jan. 1, 2018), https://cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/ [*hereinafter* EUROCLOUD].

[22] *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at 73-74 (Dec. 10, 1948); *see also* EUROCLOUD, *supra* note 21.

[23] *See* Madsen, *supra* note 20.

[24] *See* EUROCLOUD, *supra* note 21.

[25] *See* Council Directive 95/46, *supra* note 9; *see also* Elaine Burke, *GDPR and the Evolution of Data Protection*, SILICON REPUBLIC (Mar. 12, 2018), https://www.siliconrepublic.com/enterprise/gdpr-history-data-protection-ireland-eu.

[26] *See id.*

[27] *See, e.g.*, S. 5642 2019-2020, Reg. Sess. (N.Y. 2019); *see also* California Consumer Privacy Act, Cal. Civ. Code § 1798.100-198.

[28] *See* Commission Regulation 2016/679, *supra* note 10.

[29] *See* Pistorius, *supra* note 17.

[30] *See id.*; *see also* Davies, *supra* note 17.

[31] *See* Pistorius, *supra* note 17.

[32] *See id.*

privacy.[33] To date, California has received the most attention for passing a panoptic law dealing with data privacy, while the laws of some other states, such as Maine and Nevada, fail to meet the same heightened level of scrutiny as does California.[34] Many other states, prominently New York, Hawaii, Illinois, New Jersey, and Washington, have bills for proposed data privacy laws that are in committee.[35] However, these newly proposed privacy laws are not carbon copies of the GDPR and have revealed serious inconsistencies.[36]

For the remainder of this section, this note will set out a comprehensive examination of the GDPR, principally focusing on the general foundation underlying the towering GDPR, the rights of the consumers, and the duties of businesses.

B. The Mechanical Gears of the GDPR

With the focus of the Regulation shining largely on individuals' rights, the GDPR can be reduced to the treatment of two main groups; (1) the controllers or processors and (2) the data subjects.[37] Controllers of personal data must take "appropriate technical and organizational measures" in order to comply with the data subjects newfound rights under the GDPR.[38] In a nutshell, naming but a few rights and obligations, businesses must disclose that it is collecting personal information, the lawful basis under which it is authorized to collect such information, the length at which the data will be retained and stored, and the extent that it will be shared with other third parties.[39] Each of the GDPR's eleven chapters addresses a different aspect of the regulation which can be further compartmentalized into four main groups; (1) the general provisions and principles, (2) the rights of the data subjects, (3) the duties of data controllers and (4) enforcement.[40]

C. General Provisions & Principles

The GDPR, first and foremost, defines which companies are subject to the regulation.[41] With its net cast wide, any business that collects or processes personal information

---

[33] *See* Mitchell Noordyke, *State Comprehensive-Privacy Law Comparison*, INT'L ASS. OF PRIVACY PROFS. WESTIN RESEARCH CTR., https://iapp.org/media/pdf/State_Comp_Privacy_Law.pdf (last updated July 31, 2019).

[34] *See id.; see also* Kyle Schryver, *The Future of Data Privacy in the United States*, CPO MAG. (Aug. 1, 2019), https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-in-the-united-states/.

[35] *See* Noordyke, *supra* note 33 (showing that other states, such as Maine, Nevada, and California, have already enacted state comprehensive privacy laws, while bills in Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Minnesota, New Jersey, New York, Pennsylvania, Rhode Island, Texas, and Washington are either in-committee or in cross committee, and Connecticut, New Mexico and North Dakota have postponed the bill indefinitely or substituted a task force in place of a comprehensive bill).

[36] *See id.*

[37] *See* Commission Regulation 2016/679, *supra* note 10. Data controllers and data processors shall hereinafter be referred to as "Data Controllers" and "Data Processors" or "Controllers," "Processors," and collectively as "businesses" and data subjects shall be referred to individually as a "Data Subject" or "consumers" and collectively the "Data Subjects" or "consumers."

[38] *See id.*

[39] *See id.*

[40] *See id.*

[41] *See id.*

concerning a data subject residing in the EU must be GDPR compliant.[42] The GDPR, however, does not extend to individuals merely exhibiting "purely personal or household activity and thus with no connection to a professional or commercial activity."[43] While the GDPR sets broad limits for inclusion, as exhibited, for example, by the absence of a minimum threshold requirement for small to medium-sized businesses, it does impose a Data Protection Impact Assessment ("DPIA") obligation on entities that are considered "high risk."[44]

While seemingly tedious, Article 6 outlines six lawful purposes under which the collection or processing of information is permitted and complements with other provisions of the GDPR.[45] In other words, the basis under which a business collects data triggers certain rights to the consumer.[46] So long as one basis is present, lawful processing occurs.[47] All legal bases can be earmarked into one of the following groupings; (1) consent, (2) contract, (3) legal obligation, (4) vital interests, (5) public task, or (6) legitimate interests.[48]

First, when a consumer consents to the processing of her data, the scope and purpose of the company's intended uses must be disclosed through an online form.[49] A business may otherwise pinpoint a lawful basis when either (i) processing is necessary for performance of a contract with the consumer; (ii) complying with overriding legal obligations; (iii) protecting the life or vital interest of a consumer is necessary; (iv) performing an action consistent with an overriding public policy consideration; or (v) when the processing of data is of legitimate interest of the business or third party, except where the interest of fundamental human rights outweighs the benefit of the processor, specifically concerning a child's personal information.[50]

D. Rights of the Data Subject

The GDPR sets forth qualifying characteristics of what constitutes an "identifiable person."[51] This intentionally-broad definition can include "identification number, phone number, location data, or other factors which may identify that natural person," virtually

---

[42] *See id.*

[43] *Id. But see General Data Protection Regulation (GDPR),* ETSY, https://help.etsy.com/hc/en-us/articles/360001027628-General-Data-Protection-Regulation-GDPR- (last visited Nov. 5, 2019) (advising online Etsy sellers that they may need to prepare their own privacy policies and organize all data being stored offline).

[44] *See* Commission Regulation 2016/679, *supra* note 10. Further discussion on the meaning of "high risk" in context of the GDPR follows later within this note.

[45] *See id.* at art. 6.

[46] *See Lawful Basis for Processing*, INFO. COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited Jan. 27, 2020) [*hereinafter* INFO. COMMISSIONER'S OFFICE] (providing businesses with an easy-to-use interactive tool to determine whether they have a lawful basis for processing information and diagramming important interwoven interactivity of the consumers rights with Article 6).

[47] *See* Henry H. Eckerson, *GDPR Reference Guide: All 99 Articles in 25 Minutes*, ECKERSON GRP. (Nov. 28, 2017), https://www.eckerson.com/articles/gdpr-reference-guide-all-99-articles-in-25-minutes.

[48] *See* INFO. COMMISSIONER'S OFFICE, *supra* note 46.

[49] *See* Commission Regulation 2016/679, *supra* note 10, at art. 6.

[50] *See id.*

[51] *See id.* at art. 4.

making most data being collected identifiable.[52] Being that the overriding objective of the GDPR is aimed at consumer protection, data subjects are afforded an array of rights, such as (i) increased corporate transparency in the handling of consumer data—principally informing consumers—(ii) easy access to their data, and (iii) the decision to later opt-out.[53]

i. *In Plain English*

When a business extracts or stores the information of any consumer, it must inform the data subject in a "concise, transparent, intelligible and easily accessible form, using clear and plain language."[54] In other words, they cannot use overly complex and convoluted language that may mislead or confuse an ordinary person.[55] The business must also reasonably and assiduously accommodate any consumers' requests or assertions of their rights.[56]

ii. *Keeping the Consumer in the Loop*

To the average consumer, it generally remains a mystery what businesses actually do with consumer data.[57] Articles 13 and 14 attempts to flip the script by affording consumers with a right to stay informed about how their data is handled.[58] These articles require disclosure of a litany of information to the consumer once the data is obtained.[59] Walking through the flow of information, for illustrative purposes, a data controller must first provide the data subject with information about its company once it receives the consumer's information.[60] This may include disclosure of the legal basis under which it is collecting the data under Article 6 and who and how they can contact the DPO.[61] To ensure transparent processing, businesses must also inform the data subject additional details about the information, which may consist of the location of storage of data and their rights in regard to the data.[62] Then, once a consumer is legally deemed a data subject, the consumer gains an enlarged right of access, notably including the identity of any future recipient business purchasing the consumer's data.[63]

iii. *Righting a Wrong & the Right to be Forgotten*

---

[52] *Id.* at art. 12(1).

[53] *See id.* at recitals 13, 39, 66.

[54] *Id.* at art. 12.

[55] *See id.*

[56] *See id.* at arts. 12(2), 15-22.

[57] *See* Steven Melendez & Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[58] See Commission Regulation 2016/679, *supra* note 10, at arts. 13, 14.

[59] *See id.*

[60] *See id.* at art. 13(1).

[61] *See id.*

[62] *See id.* at art. 13(2).

[63] *See id.* at art. 15.

The right to recertify allows consumers to correct incorrect information contained in data records.[64] These rights, however, must be actively asserted through a formal request to amend the information.[65] While the GDPR does not define what constitutes incorrect information, it makes a general aim to protect the dissemination of inaccurate personal information that may be later used to decide eligibility for something.[66] The GDPR's right to erasure, more commonly referred to as the right to be forgotten, goes even further, allowing consumers to request the deletion of information even when accurate.[67] This opt-out provision, however, is limited to only when the scope of its processing has changed from the original scope under which it collected or in the event that the data has been processed unlawfully.[68]

iv. *Cutting the Controllers and Processors Off*

As a less drastic alternative to the right of erasure, a data subject can also request the restriction to or suppression of data in a particular manner under certain circumstances.[69] Once a data subject asserts her right to restriction, the data cannot be processed and may only be stored.[70] Further, when a business obtains a legal basis under Article 6 from consent or to perform a contract, the data subject has the right to obtain possession of a file that is "commonly used and [is in a] machine-readable format."[71] Lastly, businesses must comply with requests to transfer data to other controllers.[72]

While it may become unclear whether certain uses of data are proper, Article 21 constructs one final guardrail for consumers.[73] It gives data subjects the right to object to the usage of their information when certain instances arise, primarily when the data is being used for customer profiling or other direct marketing purposes.[74] Lastly, the use of data that is decided exclusively by an automated machine is restricted.[75]

E. Duties of Data Controllers and Processors

---

[64] *See id.* at art. 16; *see also* Case C-136/17 G.C. v Commission nationale de l'informatique et des libertés, 2019 E.C.R. 1.

[65] *See* Commission Regulation 2016/679, *supra* note 10, at art. 16.

[66] *See id.*

[67] *See id.*; *see also Right to Erasure Request Form (Template),* GDPR.EU, https://gdpr.eu/right-to-erasure-request-form/ (last visited Jan. 26, 2020).

[68] *See* Commission Regulation 2016/679, *supra* note 10, at art. 17.

[69] *See id.* at art. 18.

[70] *See* Commission Regulation 2016/679, *supra* note 10.

[71] *Id.*

[72] *See id.* at art. 20.

[73] *See* Commission Regulation 2016/679, *supra* note 10.

[74] *See id.*

[75] *See id.*; *see also, e.g., Rights related to automated decision making including profiling,* INFO. COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (last visited Oct. 13, 2019) [*hereinafter* INFO. COMMISSIONER'S OFFICE] (providing examples of restricted automated decisions such as automated loan application decisions or recruitment aptitude tests).

Chapter Four of the GDPR, specifically pertaining to the duties and responsibilities of data controllers and processors, requires that each retains accountability and ensures adequate care for the data at all times during the storage, processing, and overall possession of data.[76] Namely, controllers and processors must establish and administer technical and organizational safeguards, such as pseudonymization, anonymization, or encryption.[77]

i. DPIAs: Belt and Braces

In projects where the processing of data is classified as "high risk," controllers and processors must complete a DPIA to minimize the risk of processing the sensitive data or ensuring the protection of the data subject.[78] A DPIA essentially measures and reports the (1) scope and purpose of the collection and processing, (2) intended compliance measures, (3) risks to the data subject associated with collection and processing, and (4) measures to mitigate the potential threats and risks.[79] Although burdensome on the part of high risk controllers or processors, this measure has the power to prevent data from entering potentially dangerous hands and requires that the business have a risk mitigation plan in place prior to possessing consumer data.[80]

ii. Call to the Duty of Data Privacy: Data Protection Officer

A controller or processor is now required to appoint and maintain a Data Protection Officer ("DPO") position in its executive board.[81] This provision, however, only applies when businesses (1) are a public authority; (2) its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale; or (3) its core activities consist of processing sensitive personal data on a large scale.[82] A DPO must have "expert knowledge" of data protection laws and practices and, encompassed in her fiduciary duty to the business, must be involved "properly and in a timely manner in all issues which relate to the protection of personal data."[83] The tasks

---

[76] *See* Commission Regulation 2016/679, *supra* note 10, at arts. 24-43.

[77] *See id.* at art. 25; *see also* Kevin Moos, *GDPR Compliance: Anonymization vs. Pseudonymization*, PRIMITIVE LOGIC (May 2018), https://www.primitivelogic.com/insights/gdpr-compliance-anonymization-vs-personalization/ (distinguishing and defining anonymization as the technical coding of a data subject's personal information, making it virtually unidentifiable to the data subject, whereas pseudonymization refers to the coding of only part of the data subject's information, leaving some data still identifiable and vulnerable to cyberattack).

[78] *See Data protection impact assessments*, INFO. COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (last visited Oct. 13, 2019) [*hereinafter* INFO. COMMISSIONER'S OFFICE] (advising that when data is likely to be classified as high risk, the Processor should complete a DPIA to avoid penalty and the compromise of data).

[79] *See id.*

[80] *See id.; see also DPIA Tool*, IT GOVERNANCE, https://www.itgovernance.co.uk/shop/product/dpia-tool (last visited Jan. 28, 2020); *see, e.g. Data Protection Impact Assessment (DPIA) Policy*, UNI. OF EXETER (May 2018), https://www.exeter.ac.uk/media/level1/academicserviceswebsite/it/recordsmanagementservice/policydocuments/Data_Protection_Impact_Assessment_Policy_v1.pdf.

[81] *See* Commission Regulation 2016/679, *supra* note 10.

[82] *See id.*

[83] *Id.*

of the DPO, specifically set out by the GDPR, include informing and advising on compliance with GDPR and other EU and Member State data protection laws, monitoring compliance with the law and with the internal policies of the organization including assigning responsibilities, raising staff awareness and training staff to data privacy protocols, advising and monitoring data protection impact assessments where requested, and cooperating and acting as point of contact with the supervisory authority.[84]

iii. The GDPR's Small Break for Small Businesses

In sum, the GDPR sets a shallow bar for what is considered an "identifiable" person.[85] The data protection regulators act as the executive branch responsible for enforcing the GDPR while the European Data Protection Board is responsible for periodic review and interpretation of ambiguities.[86] Interestingly enough, the GDPR offers small businesses with less than 250 employees an exception, eliminating the painstaking Article 30 record-keeping requirement when (1) the company collects information only occasionally, (2) collection of data does not endanger the rights of data subjects, or (3) the data collected falls with the "Special Categories" designated in Articles 9(1) and 10.[87]

While difficult to cover in its entirety within the parameters of this note, hopefully, this brief explanation not provides pointed explanations of some key parts of the GDPR but also is illustrative of the subtleties looming over all businesses in the 21st century.

III. LEGAL ISSUE

One thing was certain—the inevitable US response.[88] However, the US has yet to adopt a uniform, wide-spanning law addressing the subject, while, in the meanwhile, several states have tried their hand at their own iterations.[89] Although numerous other states have adopted modern data privacy laws, this Note analyzes two American state statutes—one representing the strongest response to date, and the other the strongest pending proposal.

This section will (i) provide a broad overview of the California Consumer Privacy Act of 2018 (the "CCPA") and the pending New York Privacy Act (the "NYPA"), keying in on some of the unique features of each, (ii) highlight a few regulatory inconsistencies and inadequacies that exist between the different approaches, including the imposition of a revenue threshold qualification, right to bring a private right of action, and the inclusion or exclusion of

---

[84] *See id.*

[85] *See id.*

[86] *See id.*

[87] *See id.* at art. 30; *see also id.* at art. 9(1) (processing of information that meets a special category is prohibited, such as racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data, biometric data, health, sex life or orientation, subject to a list of exceptions); *see also id.* at art. 10 (processing of information regarding criminal convictions and offenses is prohibited).

[88] *See e.g.,* California Consumer Privacy Act, *supra* note 27; *see also, e.g.* S. 5642, *supra* note 27.

[89] *See, e.g., id.; see also* Steven Chabinsky & F. Paul Pittman, *USA: Data Protection 2019*, INT'L COMPARATIVE LEGAL GUIDES, https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa# (last visited Jan. 26, 2020).

employee data as a consumer data, (iii) conduct a cost-benefit analysis of allowing a small business exemption, and (iv) discuss the difference in cultural expectations of each society.

A. The Inevitable US Response

i. California Consumer Privacy Act of 2018

The California State Legislature signed the CCPA and it becomes enforceable in June 2020, but with the data mapping and recordkeeping requirements beginning on January 1, 2019.[90] Unlike the GDPR, however, the CCPA includes a minimum threshold requirement for small to medium-sized businesses.[91] Under the CCPA, a company falls within its regulatory orbit, thereby acceding compliance obligations under two circumstances.[92] The first, more intuitive reach of the CCPA, grabs businesses with annual gross revenues exceeding $25 million.[93] The second, albeit the more cumbersome tentacle of the CCPA, clutches businesses that either individually or collectively (i) buy data annually, (ii) receive data for commercial use, (iii) sell or share the data of at least 50,000 consumers, households, or devices for commercial purposes; or (iv) more than 50% of its annual revenues originate from the sale of consumers' personal information.[94]

While the GDPR and CCPA both have the same common goal to enhance data protection in the face of the meteoric rise of technology and data manipulation, both diverge on specific topics by taking alternative approaches, thereby creating several different denominations of data privacy protection regulations, primarily including personal scope, territorial scope, legal basis for collecting data, right not to be subject to discrimination for the exercise of rights, and the monetary penalties.[95]

While the cloak of the GDPR protects the broad category of "identifiable natural persons" and fails to specify whether the data subject must be an EU citizen, the CCPA specifically gives rights to a "consumer" defined as "a natural person who is a California resident."[96] Further, the proverbial arm of the GDPR liberally reaches all businesses that control or process data in the EU, while the CCPA delineates several qualifying characteristics that a business must meet to become subject to the law.[97] Further, relating to territorial scope, to fall within the ambit of the GDPR, a business merely needs to control or process data within the EU, regardless of whether established within or outside the EU.[98] The CCPA, on the other hand, applies to "organizations doing business in California" and essentially looks the other way when such commercial conduct occurs outside the state of California.[99]

---

[90] *See* California Consumer Privacy Act, *supra* note 27.

[91] *See id.* at subsection 140.

[92] *See id.*

[93] *See id.*

[94] *Id.*

[95] *See* DataGuidance, *Comparing privacy laws: GDPR v. CCPA*, FUTURE OF PRIVACY FORUM (2018), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

[96] *See id.*

[97] *See id.*

[98] *See id.*

[99] *See id.*

The CCPA further omits an express legal basis under which businesses can collect and process information, as seen in the staple feature of the GDPR defining and delineating several clear-cut instances under which data can be legally processed.[100] The CCPA also includes an additional consumer-faced protective provision that prevents them from being discriminated against when exercising their rights under the CCPA.[101] Under the GDPR, an offending business is subject to either (i) 2% of its global annual turnover or €10 million, whichever is higher, or (ii) 4% of its global annual turnover or €20 million, whichever is higher.[102] The CCPA, alternatively, fixes infractions at a $2,500 fine for each domestic violation and $7,500 for each international violation.[103]

ii. The New York Privacy Act

Introduced to bill on May 9, 2019, the NYPA seeks to dilate consumer protection and constrain businesses, setting a new water mark for data protection efforts, but also delineating nuances of data privacy concerns.[104] Although some argue that the NYPA is more congruent to the GDPR, going further than its sister CCPA, with the multitude of provisions contained in these laws and regulations, there is much room for variation, and each version forks in different directions.[105] The NYPA, however, still remains uncodified and in the bill, but is largely representative of the general regulatory climate that is being advanced internationally.[106] Even if the NYPA never comes to fruition, it sets a new bar for future data privacy regulation.[107]

The NYPA expands the rights of the consumers, offering them the right to recertification that is absent from the CCPA, in addition to other rights including the right to access, right to deletion, right to freeze processing, and right to have data portability.[108] While the last legislative session ended, stalling the progress of the bill in committee, it sought to go beyond the GDPR by introducing the notion of businesses acting as data fiduciaries over

---

[100] *See id.*

[101] *See id.*

[102] *See id.* Variance of the penalty percentage is based on "the nature, gravity and duration of the infringement" among other consideration included in Article 83(2).

[103] *See id.*

[104] *See* Jack Karsten & Raj Karan Gambhir, *Proposed New York bill expands scope of data privacy debate,* TECHTANK (June 24, 2019), https://www.brookings.edu/blog/techtank/2019/06/24/proposed-new-york-bill-expands-scope-of-data-privacy-debate/ (highlighting the novelty of NYPA's inclusion of an obligation on data fiduciary and ability of data subjects to personally bring a civil action against an offending data processors or collector).

[105] *See id.*; *see also* Scott Bloomberg, *Move over, CCPA? New York Considers Sweeping Data Privacy Law,* FOLEY HOAG (June 10, 2019), https://www.securityprivacyandthelaw.com/2019/06/move-over-ccpa-new-york-considers-sweeping-data-privacy-law/.

[106] *See* Lucas Ropek, *NY's Data Privacy Bill Failed; Is There Hope Next Session?*, GOV'T TECH. (July 15, 2019), https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html.

[107] *See* Robert Bateman, *New York Privacy Act vs GDPR – Which Is Tougher?*, TERMSFEED (Oct. 28, 2019), https://www.termsfeed.com/blog/nypa-vs-gdpr/.

[108] *See id.*

consumers' information, offering private recovery, as opposed to class actions, and expanding the required transparency in connection with sales data and data utilization.[109]

While the CCPA promotes the inclusion of a minimum threshold to qualify businesses based on their size and revenue, the NYPA employs broader and more stringent requirements.[110] The NYPA, although still in senate approval, more closely resembles the GDPR, chiefly in its pursuit to control all "legal entities that conduct business in New York," including those that "intentionally target" New York residents.[111]

B. Regulatory Inadequacies

The GDPR, universally regarded as the most comprehensive data privacy regulation to date, will be the subject of much future litigation and is not infallible for all intents and purposes.[112] However, the emerging patchwork state legislation arising in the US will only breed inconsistencies and future confusion and haze, thereby creating a labyrinth that is a nightmare to navigate.[113] In the technological climate that exists today, almost all businesses use and house data, some unknowingly, including mom and pop shops and entrepreneurs with storefronts on Etsy.com.[114] In short, not all data privacy laws are created equal.[115] As already illustrated, the GDPR, CCPA, and NYPA diverge at numerous points.[116] However, a few persisting and valuable differences concern (i) whether the laws should provide for sweeping applicability to businesses of all shapes and sizes, (ii) whether to allow private remedy to consumers or to exclusively government regulatory action and penalty, and (iii) whether the

---

[109] *See* Matthew Berger, *The NYPA Is Dead (for Now), But Consumer Privacy Trends Carry On*, TEALIUM (Aug. 13, 2019), https://tealium.com/blog/privacy-regulation/nypa-dead-for-now-consumer-privacy-trends-carry-on/; *see also The Indivisible Guide to the New York State Legislature*, INDIVISIBLE, https://indivisible.org/resource/indivisible-guide-new-york-state-legislature (last visited Sept. 25, 2019) (delineating that the New York Legislature begins its sessions on or around January 1, 2019 and adjourn at the end of June of the same year).

[110] *See* Joseph J. Lazzarotti, Jason C. Gavejian & Maya Atrakchi, *New York Considers Aggressive Consumer Privacy Law*, NAT'L L. REV. (June 18, 2019), https://www.natlawreview.com/article/new-york-considers-aggressive-consumer-privacy-law.

[111] *See* S. 5642, *supra* note 27; *see also id.*

[112] *See* Robert Madge, *Five Loopholes in the GDPR*, MEDIUM (Aug. 27, 2017), https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b; *see also 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 S. Comm. on the Judiciary* (2019), https://www.judiciary.senate.gov/meetings/gdpr-and-ccpa-opt-ins-consumer-control-and-the-impact-on-competition-and-innovation [*hereinafter* Statement of Layton] (statement of Roslyn Layton, American Enterprise Institute).

[113] *See, e.g.*, University of Chicago Medical Center, *Ethics study: Inconsistent state laws may complicate medical decision-making*, SCI. DAILY (Apr. 12, 2017), https://www.sciencedaily.com/releases/2017/04/170412180551.htm.

[114] *See* ETSY, *supra* note 43 (advising Etsy sellers that they may need to prepare their own privacy policies, organize all data being stored outside of Etsy, and remain transparent with the how the consumer information may be used by the Etsy seller).

[115] *See* Derrick Rice, *Data Privacy Compliance Comes to the U.S.*, TENN. CPA J. (May/June 2019), http://cdn.coverstand.com/24855/589501/21f0b6c02dc71eaab7340af66c127fa1bcb491ba.1.pdf.

[116] *See* DataGuidance, *supra* note 95; *see also* Bateman, *supra* note 107.

rights of the data subject extend to both individual consumers and employees working at a business.[117]

i. Revenue Threshold

A plurality of jurisdictions have implemented data privacy laws that broadly extend to all businesses with minimal limitations.[118] However, every path has its puddle.[119] The wide net cast by the GDPR benefits consumers with greater protection, but at the same time, these tedious and costly restrictions may unduly impair the opportunity cost associated with doing business, making it more difficult for businesses to comply, if even at all.[120] The compromise is to find a balance between the two.

With the small exception of Article 30 of the GDPR, the GDPR applies to all businesses regardless of its size.[121] While the GDPR generally does not distinguish between the sizes of companies, it does impose the DPIA requirement, which acts as a roadblock for businesses that pose a high-security risk and require additional regulatory oversight.[122] While this provision typically catches sizable businesses that process and collect plethoric data, it simultaneously subjects small businesses to the same or similar level of heightened scrutiny.[123] The NYPA sought to take a similar approach by capturing as many businesses as possible within its control.[124] The CCPA, on the other hand, takes a fundamentally unique approach, creating a minimum threshold requirement.[125]

Large corporations are mainly the culprits of data manipulation and remain the problem.[126] Small businesses, however, are consequently subject to the same standards under

---

[117] *See* DataGuidance, *supra* note 95; *see also* Karsten & Gambhir, *supra* note 104; *see also* Justine Phillips, Jessica Gross, & Daniel Masakayan, *Employee Privacy by Design: Guidance for Employers Beginning to Comply with the California Consumer Privacy Act*, SHEPPARD MULLIN (Sept. 20, 2019), https://www.laboremploymentlawblog.com/2019/09/articles/privacy/employee-privacy-by-design-guidance-for-employers-beginning-to-comply-with-the-california-consumer-privacy-act/.

[118] *See* Commission Regulation 2016/679, *supra* note 10; *see also* S. 5642, *supra* note 27.

[119] *See The Positive and Negative Implications of GDPR*, TDS, https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr (last visited Nov. 19, 2019) [*hereinafter* TDS].

[120] *See* Barry Scott, *What's in it for Consumers? The Top 5 Privacy Benefits of the GDPR*, CENTRIFY (May 30, 2018), https://www.centrify.com/blog/consumer-privacy-benefits-gdpr/; *see also* Pat Murphy, *Companies lagging in GDPR compliance, survey finds*, NEW ENG. IN-HOUSE (Nov. 25, 2019), https://newenglandinhouse.com/2019/11/25/companies-lagging-in-gdpr-compliance-survey-finds/.

[121] *See* Commission Regulation 2016/679, *supra* note 10; *see also* Felix Sebastian, *GDPR in the US: Requirements for US Companies*, TERMLY (June 21, 2019), https://termly.io/resources/articles/gdpr-in-the-us/.

[122] *See* Sebastian, *supra* note 121; *see also Data Protection Impact Assessments under the GDPR*, IT GOVERNANCE, https://www.itgovernance.co.uk/privacy-impact-assessment-pia (last visited Jan. 9, 2020).

[123] *See id.*

[124] *See* S. 5642, *supra* note 27; *see also* Bloomberg, *supra* note 105.

[125] *See* California Consumer Privacy Act, *supra* note 27, at subsection 140. To reiterate, in a nutshell, for a business to qualify for compliance adherence in California, its revenue must exceed $25 million in gross annual revenue.

[126] *See* Michael Grothaus, *How our data got hacked, scandalized, and abused in 2018*, FAST CO. (Dec. 13, 2018), https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018; *see also, e.g., In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011).

most iterations of modern data privacy laws.[127] The big-bad, big-box stores and other corporate giants have developed a global reputation for being cold and cutthroat, despite their many efforts toward positive corporate social responsibility.[128] Some supercenters, namely Walmart, have been expressly disallowed and unwelcome from certain cities due to the effects that come with its establishment.[129] The public has acknowledged that small business are enemies and often victims of big business and, in recent years, has assembled anti-corporate movements advocating for the purchase from and support of local, small businesses.[130] Although small businesses can beat out corporate giants by offering products and services with a personal edge and can more easily respond to changing conditions, big businesses inarguably have a competitive advantage over small businesses through their financial prowess, especially in industries selling homogeneous goods.[131] They have seemingly limitless resources and capital or access to such, giving them the ability to engage in price wars and poach employees with higher wages.[132] The small business movements also contribute a social dynamic to society in a way that big box stores cannot, thereby introducing a priceless social benefit within a community.[133]

On the other hand, however, some small businesses with inadequate or unsophisticated cyber security safeguards pose a different type of danger to consumers' identities, functioning as a missing link in the fence, and thereby exposing consumer

---

[127] *See* Lapowsky, *supra* note 4; *see also* Murphy, *supra* note 120.

[128] *See* Michelle Lodge, *Walmart Is Still Being Banned From One of the World's Biggest Cities, but Oddly Target Isn't*, STREET (Mar. 26, 2017), https://www.thestreet.com/story/14051569/1/walmart-is-still-being-shut-out-of-one-of-the-world-s-biggest-cities-but-oddly-target-isn-t.html. *Compare* Steven Barrison, *Study proves it: Walmart super-stores kill off local small businesses*, DAILY NEWS (May 4, 2011, 4:00 AM), https://www.nydailynews.com/new-york/brooklyn/study-proveswalmart-super-stores-kill-local-small-businesses-article-1.140129, *and* Jayson DeMers, *Amazon's Allegedly Harsh Work Culture Has Made Headlines: Here's What You Can Learn*, ENTREPRENEUR (May 7, 2018), https://www.entrepreneur.com/article/312942, *with* Kate Patrick, *Walmart's improved social responsibility efforts begin with supply chain*, INDUS. DIVE (Apr. 25, 2018), https://www.supplychaindive.com/news/walmart-corporate-social-responsibility-efforts/521961/, *and* John Dudovskiy, *Amazon Corporate Social Responsibility: a brief overview*, RESEARCH METHODOLOGY (Aug. 5, 2018), https://research-methodology.net/amazon-corporate-social-responsibility/, *and Big changes to protect the planet: Sustainability*, AMAZON https://www.aboutamazon.com/sustainability (last visited Nov. 19, 2019).

[129] *See, e.g.*, Lodge, *supra* note 128.

[130] *See* Carol Tice, *Small Business Owners – Choose Your Movement!*, ENTREPRENEUR (Nov. 8, 2010), https://www.entrepreneur.com/article/218942 (highlighting numerous small business movements such as Small Business Saturday, Independent We Stand, The Kauffman Foundation's Global Entrepreneurship Week, and Build a Stronger America, and the establishment of National Entrepreneur Day); *see also* Lisa Furgison, *Why The "Love Local" Movement is Taking Off, and How to Tap Into It*, FIVE STARS (2017), https://blog.fivestars.com/love-local-movement/ (last visited Nov. 6, 2019) (explaining that consumers "love local" businesses for their personalized services, support of the local economy, and higher quality products).

[131] *See* Devra Gartenstein, *Advantages Small Companies Have Over Large Companies*, CHRON (Mar. 4, 2019), https://smallbusiness.chron.com/advantages-small-companies-over-large-companies-23667.html. *But see* Lisa Mooney, *Does a Larger Company Always Have a Competitive Advantage?* CHRON, https://smallbusiness.chron.com/larger-company-always-competitive-advantage-36170.html (last visited Nov. 19, 2019) (stating that large corporations generally have a competitive advantage over small businesses as it relates to cost leadership, customer volume, and employee benefits and opportunities).

[132] *See* Mooney, *supra* note 131.

[133] *See* Furgison, *supra* note 130 (showing that small business movements encourage and promote local events); *see also* Eugenia Politou, Efthimios Alepis, & Constantinos Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, 4 J. OF CYBERSECURITY 1, 5 (2018).

information.[134] Both companies too large and disorganized or too small and amateurish make up the weakest links where consumer data is leaked through.

Although both of these views may be regarded as radical concerns of how the GDPR may negatively impact social and financial economies, a law or regulation as strict as the GDPR nonetheless poses a plausible handicap to small businesses, offering corporate America an additional competitive advantage over small businesses while simultaneously eroding the sense of community that exists locally and nationally.[135]

When carving out exceptions in laws and other regulatory frameworks, it is crucial to ensure that they will not be exploited.[136] This is no easy undertaking, requiring tremendous hindsight.[137] Many monolithic corporations like Walmart and Amazon are pacesetters, cautiously, but sensibly, adopting stringent data privacy protocols to get ahead of the curve, thereby minimizing any ambiguity as to their compliance.[138] Businesses that otherwise strive only to meet the minimum standard prescribed by law will routinely find themselves readjusting their data privacy protocols, and will consequently incur recurring expenses related to perfunctory reengineering.[139] As a general rule of good practice, businesses should strive to meet the most rigorous policies to avoid issues relating to compliance standards that may face legislative tightening.[140] However, at the same time, it is here that large companies gain a competitive advantage of being more financially capable of adhering to the GDPR.[141]

Small businesses may face even greater difficulty competing with larger corporations that are more equipped and capable of withstanding stringent data privacy regulations.[142] Similar to the phenomenon seen during the initial enactment of the formidable Sarbanes Oxley Act of 2002 when the cost of compliance drove public companies private, the GDPR may cause businesses to forgo participation in foreign economies due to the high cost and headache of

---

[134] *See* Allen St. John, *The Data Breach Next Door*, CONSUMER REPORTS (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

[135] *See* Kenyon, *supra* note 13.

[136] *See* Leo Katz, *A Theory of Loopholes*, 39 UNIV. OF CHI. L. SCH. 1 (2010).

[137] *See id.; see also* Madge, *supra* note 112.

[138] *See General Data Protection Regulation (GDPR) Center*, AMAZON, https://aws.amazon.com/compliance/gdpr-center/ (last visited Nov. 4, 2019); *see also Walmart Privacy Policy,* WALMART, https://corporate.walmart.com/privacy-security/walmart-privacy-policy (last updated Sept. 5, 2019). *But see* Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html; *see also* Ivana Kottasová, *These companies are getting killed by GDPR*, CNN BUS. (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

[139] *See id.*

[140] *See id.*

[141] *See* Statement of Layton, *supra* note 112; *see also, e.g.,* De Oliveira, *supra* note 16 (showing a long list of costs to comply, including, without limitation, assignment of a DPO, maintenance of a log of processing activities, gap assessment of current abilities and policies in place, revision of policies and procedures, training employees, and supervision of adherence to new policies); *see also* Oliver Smith, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown*, FORBES (May 2, 2018, 2:30 AM), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#39ea7b7534a2.

[142] *See* Statement of Layton, *supra* note 112.

complying.[143] While larger corporations have likely expended a great deal of time and resources to become GDPR compliant, it is often not an option for small businesses with business ties in the EU.[144] Smaller business, simply put, must make an economic business decision whether the cost of compliance outweighs the opportunity cost of doing business in the EU.[145] However, small and medium sized businesses are not completely thrown in at the deep end.[146] There are businesses on the market now, in fact, that aim their services towards small to medium-sized businesses who are seeking GDPR compliance.[147] Further, the GDPR website and other secondary resources provide tools, such as checklists, to become compliant.[148] Nonetheless, the question arises—is this sufficient?

Also worth mention, if businesses are hamstrung, the public may receive inferior products and services.[149] In anticipation of the enforcement of the GDPR, some companies have actively decided to offer a stripped-down version of their websites or block traffic altogether from IP addresses originating from within the EU to avoid the grip hold of the GDPR and its hefty fines.[150] Some have argued, in addition, that the expansion of data privacy laws threatens and impedes innovation as smart cities require near unadulterated access to personal consumer data to provide the best consumer experience.[151]

Therefore, considering the foregoing, while both large and small businesses are capable of causing damage that data privacy laws seek to remedy, subjecting the two to the same level of scrutiny arguably gives large businesses yet another competitive advantage over small businesses, further digging a grave for small businesses, which may cause collateral damage to sociality and innovation.[152] Accordingly, the CCPA takes a fair, balanced approach, striking an equitable reconciliation between consumer protection and business freedom of the market, rather than imposing a law characteristic of overbreadth regulation as seen in the GDPR and proposed NYPA.

---

[143] *See* David Debenham, *Going Private to Avoid Costs of Being Public – Time to Take the American SOX Off*, INBRIEF (Fall 2005), https://mcmillan.ca/Going-Private-to-Avoid-Costs-of-Being-Public--Time-to-Take-the-American-SOX-Off.

[144] *See* McAllister, *supra* note 14.

[145] *See, e.g.*, Brent Ozar, *GDPR: Why We Stopped Selling Stuff to Europe*, BRENT OZAR UNLIMITED (Dec. 18, 2017), https://www.brentozar.com/archive/2017/12/gdpr-stopped-selling-stuff-europe/ (explaining why the costs outweighed the benefits of doing business in the EU as a small business); *see also* Hannah Kuchler, *US small businesses drop EU customers over new data rule*, FIN. TIMES (May 24, 2018), https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

[146] *See* Buying into Search Engine Optimization, *supra* note 14; *see also, e.g., GDPR Defense*, SEC. METRICS, https://www.securitymetrics.com/gdpr-defense (last visited Sept. 24, 2019); *see also EU data protection rules*, EUROPEAN COMM'N, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en#abouttheregulationanddataprotection (last visited Nov. 6, 2019) [*hereinafter* EUROPEAN COMM'N].

[147] *See* Buying into Search Engine Optimization, *supra* note 13; *see also, e.g.*, SEC. METRICS, *supra* note 146.

[148] *See* EUROPEAN COMM'N, *supra* note 146.

[149] *See* Rebecca Sentence, *GDPR: Which websites are blocking visitors from the EU?*, ECONSULTANCY (May 31, 2018), https://econsultancy.com/gdpr-which-websites-are-blocking-visitors-from-the-eu-2/.

[150] *See* Kuchler, *supra* note 145.

[151] *See* Politou, Alepis, & Patsakis, *supra* note 133.

[152] *See* Julie Skeen, *Three Big Ways Businesses are Turning GDPR into Competitive Advantage: How the Investment in GDPR Compliance Can Pay Off Big*, INFOGIX (Nov. 7, 2018), https://www.infogix.com/three-big-ways-businesses-are-turning-gdpr-into-competitive-advantage/; *see also* Furgison, *supra* note 130; *see also id.*

ii. Government Regulatory Action vs. Private Remedy

If a business violates a data privacy law, the question arises as to who should have standing—society, the offended individual, or both? The differences between government regulatory action and an individual's private right to action are best exemplified by the differences between a criminal and civil lawsuit.[153] On the one hand, criminal actions are pursued by the government, or the attorney general, in the name of the society to reprimand and penalize an offender, while, on the other hand, civil actions are commenced by injured individuals seeking recovery for their damages resulting from the offender's violation.[154]

Here, in the data privacy sphere, the same is often applicable.[155] The GDPR and NYPA allow both private rights of action and actions commenced by the government.[156] However, while you can initiate a civil action in California under the CCPA, the scope of the action is generally limited to damages resulting from the breach of unencrypted data from a business's failure to set up reasonable information security practices, which leaves room for businesses to evade civil suits.[157] Ultimately, in deciding who can bring an action, it effectively determines the beneficiary of a breach—the government, the individual actually harmed, or both.[158]

Between the two courses of action, the private right of action appears to be the sensible method so that injured consumers, or the victims, have an opportunity to recover damages resulting from the violation of their rights. However, in an ideal system, the offending business should also be subject to criminal and civil penalties.[159] As in tort law, if a person is assaulted, that person can recover civil damages, and the perpetrator can be held criminally liable, which may result in a fine.[160] Although some may argue that violating businesses are thereby subject to two separate penalty schemes, which may be overly burdensome on the business, strict enforcement will force corporate compliance with the laws.[161]

iii. Rights of a Data Subject vs. Employee

---

[153] *See* Brian Duignan, *What Is the Difference Between Criminal Law and Civil Law?*, BRITANNICA, https://www.britannica.com/story/what-is-the-difference-between-criminal-law-and-civil-law (last visited Jan. 9, 2020).

[154] *See id.*

[155] *See* Bateman, *supra* note 107; *see also Recital 149: Penalties for Infringements of National Rules*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/no-149/ (last visited Jan. 9, 2020).

[156] *See* Bateman, *supra* note 107.

[157] *See Expanded CCPA Private Right of Action Fails, But Threat of Private CCPA Claims May Not Be Over*, INFOLAWGROUP (May 22, 2019), https://www.infolawgroup.com/blog/2019/5/22/expanded-ccpa-private-right-of-action-fails-but-threat-of-private-ccpa-claims-may-not-be-over.

[158] *Compare* Commission Regulation 2016/679, *supra* note 10 *and* S. 5642, *supra* note 27 *with* California Consumer Privacy Act, *supra* note 27, at subsection 140.

[159] *See* George Coppolo, *Civil and Criminal Liability of Corporate Officers and Directors*, OLR RESEARCH REPORT (Oct. 4,-2002), https://www.cga.ct.gov/2002/rpt/2002-R-0704.htm.

[160] *See* Duignan, *supra* note 153.

[161] *See e.g.*, Peter J. Henning, *Guilty Pleas and Heavy Fines Seem to Be Cost of Business for Wall St.*, N.Y. TIMES (May 20, 2015), https://www.nytimes.com/2015/05/21/business/dealbook/guilty-pleas-and-heavy-fines-seem-to-be-cost-of-business-for-wall-st.html.

It is worth emphasizing and recalling that the recent transformation of data privacy laws serves to protect consumers from businesses using their personal information for economic and commercial advantage, often without the consumer having knowledge.[162] While many privacy laws broadly reference protection of "data subjects," the identification of the members of this group is not entirely consistent across jurisdictions.[163]

The current standard under the GDPR provides for equal treatment of both employee and human resources data.[164] This means that potential or existing employees are afforded the same level of privacy protection as consumers of that business, which might seem like the correct direction for the law to be pointed.[165] However, this extension of the law may produce overlap with existing employment laws, opening up a question of preemption.[166] California's new Assembly Bill 25 dated October 11, 2019, on the other hand, modified the CCPA by excluding employee data including job applicants, employees, business owners, directors, officers, medical staff, or contractors for one year after the enactment of the CCPA, while the proposed NYPA similarly excludes employees and contractors from the statutory definition of a consumer.[167]

It should be noted that there is a longstanding and developed body of existing employment laws that already have carefully considered the factors affecting employee data privacy.[168] Interference with employment law standards may cause contradiction or may ultimately seek to reinvent the proverbial wheel.[169] However, it is possible, at the same time, that the new privacy laws may expand employees' rights and protections in the workplace beyond what is included in the current legislation.[170] The jurisprudential system may not want

---

[162] *See* Scott, *supra* note 120.

[163] *Compare* Commission Regulation 2016/679, *supra* note 10 *and* S. 5642, *supra* note 27 *with* California Consumer Privacy Act, *supra* note 27, at subsection 140.

[164] *See HR and the GDPR: Everything you need to know for HR compliance*, PEOPLEDOC, https://www.people-doc.com/hr-and-the-gdpr-everything-you-need-to-know-for-hr-compliance (last visited Jan. 9, 2020) [*hereinafter* PEOPLEDOC].

[165] *See id.*

[166] *See* Detlev Gabel & Tim Hickman, *Chapter 17: Issues subject to national law – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-17-issues-subject-national-law-unlocking-eu-general-data-protection (recognizing that "each Member State must find its own balance between the right to privacy and the requirements of national employment law").

[167] *See* California Consumer Privacy Act, *supra* note 27; *see also* S. 5642, *supra* note 27.

[168] *See e.g., Employee Privacy Rights: Everything You Need to Know,* UPCOUNSEL, https://www.upcounsel.com/employee-privacy-rights (last visited Jan. 9, 2020).

[169] *But see* Jason C. Gavejian, Joseph J. Lazzarotti, Nathan W. Austin, and Mary T. Costigan, *California Consumer Privacy Act: FAQs for Employers*, JACKSON LEWIS (Jan. 28, 2019), https://www.jacksonlewis.com/publication/california-consumer-privacy-act-faqs-employers (highlighting that the CCPA will preempt "all rules, regulations, codes, ordinances, and other laws adopted by a city, county, municipality, or local agency regarding the collection and sale of a consumer's personal information by a business" that pose a conflict or contradiction).

[170] *See Changes to employee data management under the GDPR,* TAYLORWESSING (Mar. 2017), https://globaldatahub.taylorwessing.com/article/changes-to-employee-data-management-under-the-gdpr.

to tinker with these laws by creating cross-complementing laws that overlap with the previous legislature.[171] In this vein, employee data should be separated from consumer data.

Although the GDPR functions as a more comprehensive approach to data privacy through its inclusion of employee and human resource data, this in of itself does not necessarily indicate superiority.[172] More is not always better. The paths taken in the US prescribe a cleaner, more intuitive approach to data privacy by maintaining focus primarily on consumer protection, which is the primary objective of the recent renovation of data privacy laws.[173]

C. Leveling the Playing Field

In light of these onerous regulations on business, not all businesses may have the capacity to implement these measures, highlighting the issue of whether and where a line should be drawn when considering an exemption for small and some medium-sized businesses.[174] While it is clear that billion-dollar corporate conglomerates like Walmart and Amazon should be subject to greater scrutiny as they have the resources and wherewithal to face arduous data compliance laws, small businesses are not always as capable.[175] With growing pressure exerted on small enterprises to rival tiger-competitor corporate-giants that are willing to sell below cost and engage in price wars, it is difficult to imagine that the two should be subject to the same set laws without reasonable exception.[176] It is necessary to take stock of the inconsistencies that exist between the current leading data privacy laws and to determine what approach is superior, whether in whole or in piecemeal, to Frankenstein together an even-handed and all-encompassing law that allows healthy competition and does not overly burden and potentially collapse small businesses.[177]

---

[171] *See generally* Max Rheinstein, Ulrich M. Drobnig, & Peter Hay, *Conflicts of Law*, BRITANNICA, https://www.britannica.com/topic/conflict-of-laws (last visited Jan. 28, 2020) (illustrating the common conflict of law problem).

[172] *See* Larry Clinton, *We Need Sensible Cybersecurity Regulations – More Is Not Necessarily Better*, INTERNET SEC. ALL. (June 12, 2019), https://isalliance.org/we-need-sensible-cybersecurity-regulations-more-is-not-necessarily-better/.

[173] *See* Todd S. Aagaard, *Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities*, 29 VA. ENVTL L. J. 237 (2011).

[174] *See* Pavol Magic, *How Small Businesses Can Survive in the Age of GDPR*, ENTREPRENEUR (June 27, 2018), https://www.entrepreneur.com/article/315366; *see also* Forbes Technology Council, *15 Unexpected Consequences Of GDPR*, FORBES (Aug. 25, 2018, 9:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#199708b894ad.

[175] *See, e.g.*, Ozar, *supra* note 145 (explaining why the costs outweighed the benefits of doing business in the EU as a small business); *see also* Kuchler, *supra* note 145 (highlighting that many small US companies have decided to stop conducting business abroad in the EU "rather than risk falling a foul" of the GDPR and have are actively blocked visitors originating from the EU).

[176] *See, e.g.*, Will Kenton, *Walmart Effect*, INVESTOPEDIA, https://www.investopedia.com/terms/w/walmart-effect.asp (last updated Oct. 3, 2019); *see also GDPR for Small Businesses: A Beginner's Guide*, COMPLIANCE JUNCTION, https://www.compliancejunction.com/gdpr-for-small-business/ (last visited Nov. 5, 2019).

[177] *See* Yaki Faitelson, *Data Privacy Disruption in the U.S.*, FORBES (Dec. 12, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/12/12/data-privacy-disruption-in-the-u-s/#2f198eeb15cc (highlighting that large US companies testified before the Senate on hearings for a unified data privacy law with each offering their own concoction of approaches to data privacy).

D. Different Strokes for Different Folks: Cultural Differences

Rarely are all laws applicable across borders without any cultural conflict occurring from one society to another.[178] Laws, at their very foundation, are developed and driven by the equitable expectations of the people, reflecting the cultural norms of a country.[179] The majority of the member states of the EU have a distinct sense of and appreciation for privacy from the US.[180] Exemplary of this contrast in culture, the EU formed the European Data Protection Supervisor in 2004.[181] Further to that end, in Europe, "human dignity is recognized as an absolute fundamental right" and "[i]n this notion of dignity, privacy or the right to private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role."[182] Privacy is not only an individual right but also a social value."[183]

The ultra-capitalist United States, on the other hand, lacks any uniform data privacy law or dedicated data protection authority, and its current regulatory scheme surrounding this point is mostly patchwork data breach legislation.[184] The expectation of privacy imbued by its citizens has become calloused by convenience, for example, when sharing and linking websites through Facebook or Google.[185] Some consumers deliberately choose to monetize their data privacy and allow corporate giants to purchase personal data directly from them.[186] While the GDPR's wholesome approach may be attractive on paper to some Americans, it may not necessarily fit or cater to the needs of the American lifestyle.[187] The differing attitudes and ideas surrounding privacy in US consumers, as compared to those of the EU, call for a different set of standards, and its data privacy laws should reflect the unique culture that courses through the veins of the American capitalist machine.[188] While the laws in the EU meet the cultural

---

[178] *See* Sentence, *supra* note 149.

[179] *See generally* Amir N. Licht, *Social Norms and the Law: Why Peoples Obey the Law*, 4 REV. OF L. & ECON. 715 (2008) (showing that laws closely relate to its citizens moral and social norms).

[180] European Commission Press Release IP/16/3042, The State of the Union 2016: Towards a Better Europe--A Europe that Protects, Empowers and Defends (Sept. 14, 2016), europa.eu/rapid/press-release_IP-16-3042_en.htm.

[181] *Compare* European Data Protection Supervisor, *Data Protection*, EUROPEAN UNION, https://edps.europa.eu/data-protection/data-protection_en (last visited Jan. 9, 2020) *with* Chabinsky & Pittman, *supra* note 89.

[182] *Id.*

[183] *See id.*

[184] *See Navigating the 50-State Patchwork of Data Breach Laws*, BARLEY SNYDER (Apr. 23, 2018), https://www.barley.com/navigating-the-50state-patchwork-of-data-breach-laws; *see also* Chabinsky & Pittman, *supra* note 89.

[185] *See, e.g.*, Anthony Ha, *Facebook unveils new tools to control how websites share your data for ad-targeting*, TECH CRUNCH (Aug. 20, 2019, 11:00 AM), https://techcrunch.com/2019/08/20/off-facebook-activity/.

[186] *See* Elvy, *supra* note 8; *see also* Tyler Sonnemaker, *Andrew Yang wants you to make money off your data by making it your personal property*, BUS. INSIDER (Nov. 14, 2019, 4:15 PM), https://www.businessinsider.com/andrew-yang-data-ownership-property-right-policy-2019-11?utm_content=bufferc5094&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer-ti&fbclid=IwAR1W1r9U81hgsife9umqZA5UseQOMJguWjRA8EukfMvTfi9YKIaaVNisvIg.

[187] *See* Roslyn Layton & Julian Mclendon, *The GDPR: What It Really Does and How the U.S. Can Chart a Better Course*, 19 FEDERALIST SOC'Y REV. 234 (2018) (arguing that the different regulatory approaches are influenced by the cultural norms, thereby causing variance from one country to another).

[188] *See id.*

expectations of its people, its broad application in the US may hinder the natural ebb and flow of the US economy as its cultural precepts do not emphasize data privacy in the same manner.[189]

IV. Proposed Solution

When and if the US devises a federal or uniform model law for privacy, it must take into consideration small businesses and include a minimum threshold requirement for the law to reach and take hold of larger companies.[190] Rarely are all laws absolute and without qualification.[191] Recognizing this, limiting conditions are generally included in the craftsmanship of a law to provide the most equitable of outcomes and to cushion potential parties that may be adversely affected by the imposition of a law.[192]

A. Mathematics of Regulation

Starting from the ground up, the primary purpose of regulatory laws is to protect the public from harm while balancing the burden imposed on the actor or business.[193] While there are regulations that apply to all businesses, such as minimum wage or occupational workplace safety, many regulations include thresholds that account for the size of an entity before burdening a company with additional conditions in order to conduct business.[194] Further, Professor Paul Ohm argues that regulation should not impose or apply to fixed and quantified conditions, but rather should take a spectrum-like, sliding scale approach whereby as the size of a company increases, so does the degree of its required compliance.[195]

Next after protecting the public and enforcing the societal expectations, laws must also be certain, consistent, and clear to be effective and enforceable.[196] To increase the consistency and clarity of laws, lawmakers must minimize or eliminate any overbreadth and affect only its intended offenders.[197] While ideal but rare, a law should precisely fit the exact scope and avoid making the law over or under-inclusive.[198] In this Note, it is argued that when

---

[189] *See* Bob Sullivan, *'La difference' is stark in EU, U.S. privacy laws*, NBC NEWS (Oct. 19, 2006), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/; *see also* Eric Johnson, *Why Europeans care more about data privacy than Americans*, VOX (Sept. 20, 2016, 5:14 PM), https://www.vox.com/2016/9/20/12982524/europe-data-privacy-regulation-margrethe-vestager-recode-podcast.

[190] *See, e.g.*, California Consumer Privacy Act, *supra* note 27.

[191] *See* Paul Ohm, *Regulating at Scale*, 2 GEO. L. TECH. REV. 546, 547-48 (2018); *see also* Henry Kenyon, *Draft GDPR legislation mulled over by Polish government*, CQ ROLL CALL (Jan. 29, 2018) (exemplifying that other EU member states have considered including a small business exemption).

[192] *See* Ohm, *supra* note 191.

[193] *See id.*

[194] *See id.*

[195] *See id.*

[196] *See* Randall J. Cude, *Beauty and the Well-Drawn Ordinance: Avoiding Vagueness and Overbreadth Challenges to Municipal Aesthetic Regulations*, 6 J. OF L. AND POL'Y 853 (1998); *see also* Patricia Popelier, *Legal Certainty and Principles of Proper Law Making*, 2 EUR. J. OF L REFORM 321 (2000).

[197] *See id.*

[198] *See* Legislative Research Council, *Guide to Legislative Drafting*, S.D. LEGISLATURE (2019), http://sdlegislature.gov/docs/referencematerials/draftingmanual.pdf.

creating new data privacy laws, the legislature must find a happy medium between the encroachment on the public's data privacy and the cost of compliance for smaller businesses to compete with larger companies.

B. Suggested Approach

The most practical resolution would be the drafting of a uniform act or model act.[199] Model laws offer a multitude of benefits, including the resolution of inconsistencies that can cause preemption issues, the wealth gained from uniformity, and the ease in gaining widespread acceptance.[200] While drafting an entire model code would exceed the parameters of this Note, its ideal effect would serve as a catalyst, igniting the spark that influences the equitable drafting of a comprehensive model code tailored to the current data privacy threats that face the public.

i. *Revenue Threshold*

The approach taken by the CCPA offers a pragmatic solution in consideration of the challenges that small businesses face in light of stringent data privacy regulations that comport with the culture present in the US.[201] However, the GDPR brings about a semi-sliding scale approach by imposing its DPIA requirements on business as they become a more significant risk, which is often associated with the volume of data processed.[202] An alternative and arguably superior approach would be to formulate a hybrid between the two—defining a minimum threshold requirement while also imposing additional, stricter specifications as the volume of data processed by and the size of a company grows.

While it may be perceived as presumptuous and grandiose, this Note structures a proposed small business exception that tailors to the cultural needs and expectations of the surrounding society. This Note urges consideration when, and if, the drafting of broad span federal data privacy law occurs. While the CCPA set a minimum threshold for businesses earning $25 million in revenue, this still allows for many businesses, perhaps more than would be necessary, to bypass data privacy laws.[203] Current revenue statistics indicate that the average small business owner earns $71,813 annually, which remains well below CCPA's minimum threshold.[204] With 89% of businesses having less than 20 employees in the US and 81% of

---

[199] *See Model Legislation*, AM. ACADEMY OF FAMILY PHYSICIANS, https://www.aafp.org/advocacy/states/model-legislation.workforce.0.html (last visited Jan. 30, 2020).

[200] *See Overview*, UNIF. LAW COMM'N, https://my.uniformlaws.org/aboutulc/overview (last visited Jan. 27, 2020).

[201] *See CCPA for Small Business: Considerations from the New California Privacy Law*, CLARIP, https://www.clarip.com/data-privacy/ccpa-small-business/ (last visited Nov. 19, 2019).

[202] *See* Ben Oster, *Dirty Little Secrets: A "Word" on Privacy Impact Assessments (PIAs)*, AVEPOINT (Jan. 11, 2017), https://www.avepoint.com/blog/technical-blog/dirty-little-secrets-word-wise-privacy-impact-assessments-pias/.

[203] *See* Nina Godlewski, *Small Business Revenue Statistics (2020): Annual Sales and Earnings*, FUNDERA, https://www.fundera.com/resources/small-business-revenue-statistics (last updated Dec. 31, 2019).

[204] *See id.* (stating that "[i]n 2007, businesses with one to four employees averaged $387,000 in revenue per year, while those with five to nine employees averaged $1,080,000. And the numbers continue to increase from there: Small businesses with 10 to 19 employees averaged $2,164,000 in revenue, those with 20 to 99 employees averaged $7,124,000, and coming in on top are companies with 100 to 499 employees averaging $40,775,000 in revenue").

businesses with no employees, according to the latest US Census Bureau statistics, most businesses escape the CCPA.[205]

First, the threshold amount should be reduced to a level so that only small businesses remain unaffected, excluding mid-sized businesses. The approach may become more nuanced through the use of a similar system analogous to the DPIA device used in the GDPR.[206] As a company grows in the level of risk, climbing requirements should be imposed through consideration of, but not limited to, the volume of data being processed, the sensitivity of the information collected, and its information systems and technology security systems, such as secure server and communications measures.

ii. *Private Right of Action*

To briefly recap, the GDPR and NYPA allow both private rights of action and actions commenced by the government.[207] Interestingly, however, a divide exists between the New York and California approaches.[208] While the initiation of a CCPA civil action in California is possible, the scope of the action is limited, leaving wiggle room for businesses to circumvent civil suits.[209] From an objective standpoint, this corporate consideration is antithetical to the purpose of these newfound data privacy laws—protecting the consumer.[210] Further, the possibility for businesses to be subject to two actions, resulting in separate fines will also impart firmness of and subsequent adherence to the law.[211] In the drafting of a model act, therefore, the Uniform Law Commission should permit the pursuit of both consumers' and the government's claims against businesses that offend data privacy laws.

iii. *Employee Data as Consumer Data*

Currently, the GDPR offers equal treatment to both employee and human resources data while the CCPA and the proposed NYPA exclude employee data from the reach of its data privacy laws.[212] The definitional division between an employee versus a consumer is a worthwhile one.[213] Severance of employee data from an already broad spanning data privacy

---

[205] *See U.S. Census Bureau Releases 2017 Economic Census First Look Estimates*, U.S. CENSUS BUREAU (Sept. 19, 2019), https://www.census.gov/newsroom/press-releases/2019/economic-census-first-look.html; *accord* Janet Attard, *How much do small businesses really earn?*, BUS. KNOW-HOW, https://www.businessknowhow.com/money/earn.htm (last updated Jan. 21, 2020).

[206] *See* INFO. COMMISSIONER'S OFFICE, *supra* note 78.

[207] *See* Bateman, *supra* note 107.

[208] *See* Robert Bateman, *New York Privacy Act v. California's Privacy Laws*, TERMSFEED (Nov. 22, 2019), https://www.termsfeed.com/blog/nypa-vs-california-privacy-laws/.

[209] *See* INFOLAWGROUP, *supra* note 157.

[210] *See Data Privacy in the United States: Current Legislation and Predictions*, FORMASSEMBLY (Nov. 14, 2019), https://www.formassembly.com/blog/data-privacy-united-states-ccpa-law/.

[211] *See* Coppolo, *supra* note 159.

[212] *See* PEOPLEDOC, *supra* 164; *see also* California Consumer Privacy Act, *supra* note 27; *see also* S. 5642, *supra* note 27.

[213] *See* email from Fernando, public comment letter writer, to Xavier Becerra, California Attorney General, (Oct. 18, 2019, 3:17 PM) (on file with Office of the Attorney General in State of California Department of Justice), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day-pt1.pdf (urging CA government to

law will outweigh the marginal loss experienced by employees, primarily considering the anti-conflict and preemption avoidance features of its division.[214] While the grouping of the two distinct categories may be intuitive abroad, the room for error and accidental overlap warrants division in the US.[215] As supported by state legislatures of California and New York, a US model code should too make this distinction.[216]

V. CONCLUSION

The GDPR is undoubtedly morphing the way in which business is conducted in the Information Age.[217] From mom and pop shops to big box stores, the effect have become widespread.[218] Some governments have decided to treat the two as equal when enforcing the laws, while others have offered some leniency to smaller businesses.[219] It is worth noting that data privacy laws and regulations may have the capability of thwarting the free, unrestricted flow of data that is reminiscent of the early Information Age of information.[220] If arduous and complex regulations encumber small businesses, many have and will forego the motions of complying with the laws altogether, which will likely have an adverse and detrimental effect on the economy.[221]

Overregulation is a problem, and it is noteworthy that the intended scope of data privacy regulation remains unobscured by unnecessarily convoluted legislation.[222] The goal here is to protect consumers, but at a cost that is reasonable and digestible to companies so that business is not unduly thwarted.[223] In the end, however, the cost of GDPR or a like-data privacy device will likely be added to the price tag of a product or service like a service charge or an automatic gratuity included in the restaurant bill.[224] The business may displace its GDPR

---

exclude employee information from the grasp of the CCPA because it is unduly burdensome on businesses); *see also* California Consumer Privacy Act, *supra* note 27 (including an amendment, through its AB 25, clarifying that employee data is excluded from the meaning and reach of the CCPA).

[214] *See generally* Sean Paisan, *California Amends CCPA, Imposing Fewer Requirements on Employee Data Prior to January 1, 2020*, NAT. L. REV. (Oct. 16, 2019), https://www.natlawreview.com/article/california-amends-ccpa-imposing-fewer-requirements-employee-data-prior-to-january-1 (reporting that California amended the CCPA by limiting employee coverage under the CCPA, which supports the inference that California found it necessary to impose fewer requirements on businesses with respect to employee data).

[215] *See* Aagaard, *supra* note 173; *see also* Layton & Mclendon, *supra* note 187.

[216] *See* S. 5642, *supra* note 27; *see also* California Consumer Privacy Act, *supra* note 27.

[217] *See* Peter Zaffino, *Commentary: These New Regulations Could Transform U.S. Corporate Titans*, FORTUNE (Feb. 6, 2018), https://fortune.com/2018/02/06/gdpr-general-data-protection-regulation-eu-compliance/; *see also* GDPR & BEYOND, https://www.gdprandbeyond.com/ (last visited Nov. 19, 2019).

[218] *See id.*

[219] *Compare* Commission Regulation 2016/679, *supra* note 10 *and* S. 5642, *supra* note 27 *with* California Consumer Privacy Act, *supra* note 27.

[220] *See* James Wickes, *Why Life Under GDPR will Encourage Technology Innovation*, INFOSEC. (June 21, 2018), https://www.infosecurity-magazine.com/opinions/gdpr-encourage-technology/.

[221] *See, e.g.*, Ozar, *supra* note 145; *see also* Kuchler, *supra* note 145.

[222] *See* TDS, *supra* note 119.

[223] *See id.*

[224] *See* Angelique Carson, *Should vendors be able to pass along costs of GDPR compliance?*, INT'L ASS'N OF PRIVACY PROF'LS (Aug. 28, 2018), https://iapp.org/news/a/should-vendors-be-able-to-pass-along-costs-of-gdpr-compliance/.

compliance cost, essentially leaving the customer footing the bill for its privacy, without choice, revealing a larger question that challenges the premise of a free marketplace.[225]

As one final consideration—for the most part, US consumers will gloss over the countless contracts they enter on the Internet, blindly signing away their rights. It will be interesting to examine the practicality of data privacy laws in the US by observing how many consumers actually make use of their newfangled rights. The effort required from the consumer may outweigh the consumer's inherent value for data privacy. Will it work in the United States? Do Americans really care? In the very least, Americans will undoubtedly gain leverage over large businesses hungry for organic data, establishing a market for consumers to profit from their data and conferring a pecuniary power to the public.[226]

Not all laws are created or imposed equally, with some protecting smaller business operations.[227] Large corporations and small businesses are far from competing on the same playing field, and the clutches of contemporary data privacy laws should not make that assumption.[228] Most laws are intended to satisfy the needs of the different cultures of their respective countries, and therefore, a one-size-fits-all approach will not work.[229]

---

[225] *See id.*

[226] *See* Sonnemaker, *supra* note 186.

[227] *See* Rice, *supra* note 115; *see, e.g.,* 26 U.S.C. §163(j)(3).

[228] *See* Magic, *supra* note 174.

[229] *See* Layton & Mclendon, *supra* note 187.