UC Irvine Law Review

Volume 10 | Issue 4 Article 11

6-2020

The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act

Grace Park

The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act

Grace Park*

On May 25, 2018, the European Union's (EU) General Data Protection Regulation (GDPR) came into effect. The GDPR is expected to reshape web use and overhaul data privacy laws beyond Europe in how businesses and organizations can handle customer and user information. Only a month after, California passed the California Consumer Privacy Act of 2018 (CCPA). The CCPA is one of the most significant regulations overseeing data-collection practices of businesses in the United States. It is the first of its kind and is expected to provide the most comprehensive data privacy measures in the United States. As such, the combined CCPA and GDPR data privacy regulations will likely usher in a tidal wave of changes, most likely setting new data privacy standards for other jurisdictions to model.

Drawing from these events, this Note will examine the EU's and California's newest data privacy laws, studying the immediate and potential effects of GDPR and CCPA regulations on the existing data privacy regime. Through a comparative study of GDPR and CCPA provisions, this Note attempts to answer key questions in discourse today—to what extent are the CCPA and GDPR moving towards convergence or divergence, and how will the laws affect businesses and consumers? Is the U.S. data privacy environment veering away from its hands-off approach and drawing closer to the comprehensive approach of the EU data privacy regime? This Note will explore these questions looking at two particular provisions in the GDPR and CCPA: (1) the opt-in vs. opt-out consent and (2) the right to be forgotten/right to delete personal data.

Lastly, this Note analyzes the practical implications of the GDPR and CCPA regulations on businesses in terms of how receptive businesses are to the regulations, how well businesses strive to conform to the regulatory boundaries of data privacy regimes, and whether the regulations will have the intended effect of strengthening consumer rights by putting heavier restrictions on businesses.

---

* Ms. Grace Park is a member of the Class of 2019 of the University of California, Irvine School of Law. Many thanks to Professor David Kaye for his guidance and suggestions to pursue and research this topic.

INTRODUCTION

The year 2018 was a huge step forward for advocates who have long pushed for stronger data protection for individuals. On May 25, 2018, the EU's General Data Protection Regulation (GDPR) came into effect with fanfare, as businesses and organizations impacted by the law scrambled to meet the new benchmark for data protection. The GDPR is expected to reshape web use and overhaul data privacy laws beyond Europe, altering how businesses and organizations can handle customer and user information. Coming on the heels of GDPR's effective date, the California state legislature hastened to pass the California Consumer Privacy Act of 2018 (CCPA) a month later. The CCPA is one of the most significant regulations overseeing data-collection practices of technology companies in the United States.[1] Going into effect in January 2020, the California law is the first of its kind in the United States and is expected to provide the most comprehensive data privacy measures in the United States. The CCPA is being closely watched because California has been a forerunner in enacting various laws protecting consumer rights. Data privacy rights are no different. The combined CCPA and GDPR data privacy regulations will likely usher in a tidal wave of changes because these initiatives are being carried forth by the world's major economic powers[2] and will most likely set new data privacy standards for other jurisdictions to model.

---

1. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/4R83-SVZD].

2. *See* Kieran Corcoran, *California's Economy Is Now the 5th-Biggest in the World, and Has Overtaken the United Kingdom*, BUS. INSIDER (May 5, 2018), https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5 [https://perma.cc/2S4B-GYN6].

The focus on laws fortifying data protection comes at the same time that 2018 became the year that consumers intensified demands for greater corporate accountability. Reports after reports of massive data breaches or privacy intrusions have come to light. In March 2018, news broke that Cambridge Analytica had collected and sold personal data of millions of Facebook users without their knowledge or consent. In August 2018, a user sued Google after reports emerged of Google Maps storing users' location data even when "Location History" was turned off.[3] One month later, Facebook revealed that hackers had breached and gained access to more than thirty million users' personal data.[4] Most recently, investigation by the Irish Data Protection Commissioner divulged information that Microsoft's LinkedIn professional networking application ("app"), i.e., a software program run on computers or mobile devices to perform specific tasks, misused email addresses of eighteen million nonmembers in the United States.[5] According to reports, LinkedIn used the emails to get more people to sign up for the service by using them in hashed form to place targeted ads on Facebook's platform.[6]

The constant media stream of corporations mishandling personal data has steadily contributed to the growing awareness of Internet privacy issues. Users are "very concerned" about companies like Facebook that have failed to institute policies safeguarding personal data and have indeed profited from the misuse of users' personal data.[7] Thus, recent events have united voices calling for stronger data protection regulation to the forefront of national discourse. The public seems to be at a turning point in what it expects governments to do in order to curb corporate misuse of personal data and strengthen data privacy laws to protect consumer rights.[8]

Accordingly, this Note conducts a study into the EU's and California's newest data privacy laws in order to examine the immediate and potential effects of the GDPR and CCPA regulation on the existing data privacy regime. This Note will compare and analyze where the GDPR and CCPA provisions align and where they

---

3. Cyrus Farivar, *Man Sues Over Google's "Location History" Fiasco, Case Could Affect Millions*, ARS TECHNICA (Aug. 20, 2018, 10:55 AM), https://arstechnica.com/tech-policy/2018/08/did-google-violate-users-privacy-when-it-secretly-kept-location-data/ [https://perma.cc/N5CK-QRNT].

4. Allen St. John, *Facebook Breach Exposed Personal Data of Millions of Users*, CONSUMER REPORTS (Oct. 12, 2018), https://www.consumerreports.org/digital-security/facebook-data-breach-exposed-personal-data-of-millions-of-users/ [https://perma.cc/3RQ4-4QRW].

5. Alan Friedman, *Ireland's Data Protection Commissioner Says LinkedIn Misused Data from 18 million Non-Members*, PHONEARENA.COM (Nov. 25, 2018, 12:45 PM), https://www.phonearena.com/news/LinkedIn-wrongly-used-18-million-email-addresses-for-a-subscription-drive_id111332 [https://perma.cc/MD52-AZDD].

6. *See id.*

7. *See* Justin McCarthy, *Worries About Personal Data Top Facebook Users' Concerns*, GALLUP (Apr. 12, 2018), https://news.gallup.com/poll/232343/worries-personal-data-top-facebook-users-concerns.aspx [https://perma.cc/37XJ-6BK8]; *see also* Brian Byer, *Internet Users Worry About Online Privacy but Feel Powerless to Do Much About It*, ENTREPRENEUR (June 20, 2018), https://www.entrepreneur.com/article/314524 [https://perma.cc/37XJ-6BK8].

8. *Public Opinion on Privacy*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/survey/ [https://perma.cc/47WK-X3LW] (last visited Nov. 21, 2019).

diverge, drawing important conclusions about data privacy regulation in California and the EU, and the potential regulatory effect on businesses and consumers. The Note begins by tracing the development of Internet and privacy law, providing an overview of the United States' and the EU's conceptualization and implementation of data privacy laws over time. Part II examines particular provisions in the GDPR and CCPA, namely clauses related to (1) the opt-in vs. opt-out consent and (2) the right to be forgotten. This Note attempts to answer key questions in discourse today—to what extent are the CCPA and GDPR moving towards convergence or divergence, and how will it affect businesses and consumers? The CCPA will serve as a case study to determine whether the U.S. data privacy environment is veering away from its hands-off approach and drawing closer to the comprehensive approach of the EU data privacy regime. Lastly, this Note will draw practical implications of the CCPA and GDPR regulations on businesses in terms of how receptive businesses are to the regulations, how well businesses strive to conform to the regulatory boundaries of data privacy regimes, and whether the regulations will have the intended effect of strengthening consumer rights by putting heavier restrictions on businesses.

I. THE DATA PRIVACY FRAMEWORK

A. What is Data Privacy Law?

Data privacy is an area of law that involves (1) *personal* data and (2) the control over how personal information is collected and used.[9] Personal data concerns "personally identifiable information," such as an individual's name, address, phone number, employment location, credit card number, social security number, and other identifying elements with which another individual could act as though she were that person.[10] The terms *data privacy* and *data protection* are often used interchangeably; in reality, they can have very different meanings depending on the jurisdiction, industry, or market sector.

Data privacy refers to the appropriate use of personal information under the circumstances, depending on the legal context, individual's expectations, and the individual's right to control over the information.[11] Data protection relates to the

9. LUKAS FEILER, INFORMATION SECURITY LAW IN THE EU AND THE U.S.: A RISK-BASED ASSESSMENT OF REGULATORY POLICIES 11 (2012); *see also What Does Privacy Mean?*, *About the IAPP*, IAPP, https://iapp.org/about/what-is-privacy/ [https://perma.cc/CCR2-7P95] (last visited Nov. 21, 2019).

10. Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693, 695–96 (2007).

11. *What Does Privacy Mean?*, *supra* note 9; *see also* FORBES TECH. COUNSEL, *Data Privacy vs. Data Protection: Understanding the Distinction in Defending Your Data*, FORBES (Dec. 19, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#58bfba1150c9 [https://perma.cc/EQ4M-X9SE].

management or technical control of personal information.[12] Data privacy is about authorized access—who has access to the personal information and who defines it; data protection is about securing data against unauthorized access.[13] United States law typically groups laws and regulations covering the management of personal information under privacy law.[14] By contrast, the EU refers to data protection for privacy-related laws and regulations.[15] These distinctions lead to legal differences in how the CCPA and GDPR define "personal information," which warrants a separate discussion beyond the scope of this Note. This Note uses the term "data privacy" to discuss general privacy-related laws in the EU and the United States. Data protection is used only in the context of discussions regarding existing EU laws and regulations and GDPR provisions.

Privacy laws promote the growth of electronic commerce ("e-commerce"). Privacy laws are designed to protect consumers worried about identity theft from unwanted exposure of private information to strangers or the government.[16] The statistics on Internet data traffic are staggering; over 4.1 billion Internet users spend over $2.84 trillion on online retail sales, and conduct over five billion Google searches daily around the globe today.[17] As a result, it is in the interest of governments, businesses, and consumers for privacy laws to be clearly delineated in order for those involved to responsibly use and access personal data and associated activities.

For e-commerce to work, both online companies and Internet consumers must be willing to disclose information about themselves. Disclosure of personal data is also necessary for Internet users to set up and browse through social media accounts. Many users willingly offer more detailed personal information in order to customize and personalize their individual social media platforms, commercial transactions, and news consumption.

Businesses can obtain customer information online in two ways: (1) through willing disclosure or (2) through other indirect means of disclosure that users are less aware of.[18] A willing disclosure is made when a consumer visits a website and voluntarily registers or provides personal information to the company, which captures and retains the information.[19] This transaction not only provides personal information, but it also inadvertently supplies information related to the consumer's

12. *See* FORBES TECH. COUNSEL, *supra* note 11.

13. *Id.*

14. Rick Robinson, *Data Privacy vs. Data Protection*, PROGRESS (Jan. 30, 2020), https://blog.ipswitch.com/data-privacy-vs-data-protection [https://perma.cc/5EYW-P94T].

15. *Id.*

16. CLARA RUYAN MARTIN & DAVID B. OSHINSKY, INTERNET LAW AND PRACTICE IN CALIFORNIA § 9 (2019).

17. *Internet Stats & Facts for 2019*, HOSTING FACTS (Dec. 17, 2018), https://hostingfacts.com/internet-facts-stats/ [https://perma.cc/7N78-8N38].

18. MARTIN & OSHINSKY, *supra* note 16, § 9.3(1).

19. *See id.*

preference and personal habits.[20] Other information that may be shared willingly is location data and biometric data, such as facial, fingerprint, and iris information.[21] Alternatively, businesses obtain user information through indirect means of disclosure by mining data through the use of cookies, web bugs, or tracking software.[22] Monitoring internet protocol (IP) addresses is one way to collect data.[23]

Businesses mine data in exchange for providing the public with useful products, and they use the metadata to enhance and deliver those products more efficiently to the consumers who desire them.[24] This second means of obtaining information is less obvious, and therefore, average Internet users are less aware of this type of information exchange. Surveys suggest that half of the survey respondents falsely believe online tracking is unlawful and a majority of consumers are not willing to allow companies to mine data *with permission* in exchange for free product or service.[25] The notion that the business practice of mining data is violative of privacy principles—reaching a level of deception and manipulation for companies using the data to take advantage of consumers' cognitive biases and propel them to act in ways harmful to their self-interest—has gained traction over the years.[26]

Businesses and governments recognize the importance of retaining "consumers' trust in the technologies and companies that drive the digital economy" as much as they emphasize the need to promote innovation.[27] Given the role of trust in facilitating the disclosure of information online,[28] governments have a keen interest in ensuring consumer confidence in the Internet. Moreover, erosion of trust is a central concern for Internet users seeking greater corporate accountability for data privacy breaches.[29] A survey conducted in 2018 asked over 700 U.S. adults a question—how much risk do you believe theft or exposure of private data poses to human health, safety, or prosperity?[30] More than seventy percent of the respondents rated the risk above moderate and almost fifty percent rated it high or very high.[31] Following numerous reports of corporate misuse or

20. *Id.*

21. *Id.*

22. *Id.* § 9.4(2).

23. *Id.*

24. Nancy S. Kim & D.A. Jeremy Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent*, 80 MO. L. REV. 723, 729 (2015).

25. *Id.* at 738–39.

26. *Id.* at 744.

27. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 31–32 (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/MFK5-MEJA].

28. Miriam J. Metzger, *Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce*, 9 J. COMPUTER-MEDIATED COMM. (2004).

29. *Id.*

30. Stephen Cobb, *Data Privacy vs. Data Protection: Reflecting on Privacy Day and GDPR*, ESET: WELIVESECUTIRY (Jan. 25, 2018, 1:58 PM), https://www.welivesecurity.com/2018/01/25/data-privacy-vs-data-protection-gdpr/ [https://perma.cc/X7C8-LHPV].

31. *Id.*

mishandling of data this year, the level of mistrust among Internet users is likely to have exceeded prior levels. At the same time, no amount of mistrust is likely to push people completely offline because the world has become so dependent on the Internet for the purposes of extracting information and communicating online for personal enjoyment, livelihood, and professional work. As a result, instituting prophylactic measures for data privacy has become a growing necessity.

B. The Development of Internet Law

Although the United States and Europe do not share similar regulatory climates on data protection, they have historically shared a commitment to an individual-oriented understanding of privacy. This rights-based concept of data privacy was first embodied in the code of Fair Information Practices (FIP), first proposed by the U.S. Advisory Committee on Automated Personal Data Systems in 1973 on behalf of the Department of Health, Education, and Welfare.[32] The FIP served as a model for the U.S. Privacy Act of 1974 in the wake of the Watergate scandal. The FIP also later formed the core of the EU's data protection laws, codified at the Council of Europe's 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data—"the first legally binding international instrument in the field of data protection"—as well as the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) and the EU's 1995 Data Protection Directive.[33] Therefore, the FIP was an instrumental expression in shaping the individual rights–based approach to privacy rights in the United States and the EU.

The FIP approach relies on procedural protections, as illustrated in the OECD Guidelines—the most influential statement of the FIP.[34] The OECD Guidelines consider privacy protection in relation to personal data to prevent violations of fundamental human rights, such as the unlawful storage of personal data, the storage

32. The Committee was appointed by the Department Secretary to assess the impact of computer-based record keeping on private and public matters and recommended safeguards against its potentially adverse effects. See KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 21 (2018), in reference to SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/L5NZ-WBRQ].

The major principles of the code include: (a) transparency of personal data collected for use; (b) individual right to find out what information is collected about him and how it is used; (c) limitations on the use of information obtained for one purpose to be used for other purposes without his consent; (d) individual right to correct or amend a record of identifiable information about him; and (e) the responsible and reliable use of data collected by any organization creating, maintaining, using, or disseminating records of identifiable personal data precautions to prevent misuse of the data.

33. BAMBERGER & MULLIGAN, *supra* note 32, at 21.

34. *Id.* at 22.

of inaccurate personal data, or the abuse or unauthorized disclosure of such data.[35] The OECD Guidelines articulate principles in detail such as individual control over personal information, transparency and accountability of data collection and use, limitations and security of data collection, and user access to accurate personal information.[36] But according to Bamberger and Mulligan, the FIP model often fails. The FIP model reduces privacy protection to "legalistic principles (e.g., notice, choice, access, security, and enforcement)" and has thus been criticized as insufficient to address concerns raised by technological developments, changing risks, and globalization.[37] This has led to a technical and social trend suggesting "an increasing reliance on consent globally."[38]

Within the FIP model of data protection, privacy is the core protected interest, and individual consent is the central vehicle through which this protection is accomplished.[39] The principle of consent is linked to the law of contracts, which is a form of self-regulation and an expression of autonomy.[40] Internet governance by contract is a regime in which contracts provide the glue for an agreement between actors who voluntarily coordinate to enable efficient data transfer, exercise control, create or reinforce a sense of community, and set down fundamental rules for the governance of a digital community.[41] Contractual agreements usually provide boilerplate clauses, are formulated in legalese, and are adhesive in nature.[42] This is problematic for contract theorists who believe consumers need to meaningfully consent to the terms of an agreement through an arm's-length negotiation and reach a customized agreement.[43] However, standardized deals lower information costs and are more efficient when applied to mass-market, high-volume, and low-value transactions such as the Terms of Use, Terms of Service, and End User License Agreements that businesses and consumers enter into on the Internet.[44]

The origin of contracts as the basis of Internet governance derived from the American laissez-faire ideology and the freedom of expression.[45] At the developmental stages, the U.S. government supported the nascent growth of Internet community characterized by a bottom-up decisional culture of the

35. *Part 1. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, General Definitions* and *Part 2. Basic Principles of National Application*, of *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD (Sept. 23, 1980), https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/8JZ5-KT8P].

36. BAMBERGER & MULLIGAN, *supra* note 32, at 22.

37. *Id.* at 23.

38. *Id.* at 23.

39. Lisa M. Austin, *Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA*, 56 U. TORONTO L.J. 181, 181 (2006).

40. LEE A. BYGRAVE, INTERNET GOVERNANCE BY CONTRACT 23 (2015).

41. *Id.* at 39.

42. *Id.* at 40.

43. *Id.*

44. Joshua Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1401, 1405, 1407 (2009).

45. BYGRAVE, *supra* note 40, at 44.

network's technical pioneers.[46] This meant that the development of the Internet and the networks that grew out of it had a horizontal growth, not a top-down approach.[47] Bygrave goes so far as to state that "lawmakers who are unappreciative of the social conditions that foster informal cooperation are likely to create a world in which there is both more and less order."[48] This type of informal, consensus-based governance framework faded into the background as the Internet became more fragmented by geography, and governments began to employ top-down techniques to control unwanted Internet communications from abroad.[49] Yet, Internet governance by contract and the notion that "a click constitutes a 'manifestation of assent'" still remain powerfully relevant because it serves as the basis for many popular and widely-used Internet programs, especially those dominated by the Big Five technology companies—Apple, Alphabet/Google, Facebook, Microsoft, and Amazon.[50]

Yet, researchers have paradoxically found that increasing individual control over personal information such as provision of privacy notices and more granular controls over data use leads individuals to disclose more sensitive information.[51] The vast majority of Internet consumers rarely read or browse Terms of Service (TOS). In a widely circulated story, Game Station, a computer game retailer, included a term describing the company's right to claim the "souls" of 7,500 of its online customers, but many of its users failed to nullify this term by simply checking a box to opt-out, which would have also rewarded the users with a five pound voucher.[52]

At the same time, critics point out that organizations attempt to structure compliance with regulations in ways that most easily achieve the appearance of legitimacy. Accordingly, companies focus on easily visible indicators of compliance through a "check-the-box" approach to compliance.[53] So then, a "contract serves as a powerful legitimizing tool for companies and may convince consumers, ex-post [in]formation, to shift responsibility away from the companies engaging in dubious practices and toward users for failing to read and understand terms to which they 'consented.'"[54] Moreover, a privacy regime that relies on self-regulation through the use of contracts to obtain individual consent does not necessarily provide comprehensive legal rights to the individuals concerned. But individuals have

46. *Id.* at 46.

47. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 24 (2006).

48. BYGRAVE, *supra* note 40, at 46.

49. GOLDSMITH & WU, *supra* note 47, at 49.

50. Kim & Telman, *supra* note 24, at 734; *see* Conor Sen, Opinion, *The 'Big Five' Could Destroy the Tech Ecosystem*, BLOOMBERG: OPINION (Nov. 15, 2017, 8:00 AM), https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem [https://perma.cc/4CBS-E5KH].

51. BAMBERGER & MULLIGAN, *supra* note 32, at 23.

52. Kim & Telman, *supra* note 24, at 733.

53. BAMBERGER & MULLIGAN, *supra* note 32, at 28.

54. Kim & Telman, *supra* note 24, at 736.

legitimate interests in their privacy and over the security of their personal information, irrespective of whether privacy is protected by government regulation or only self-regulation.[55]

The preceding overview of the differing type of Internet law and critiques of the existing systems encapsulate some of the debate surrounding the current regulatory approaches of the EU and California data privacy laws, as well as the legislative intent and probable effects of the GDPR and CCPA regulations of individual data privacy rights.

C. Data Privacy Regulatory Environment in the United States and the European Union

The regulatory environments of the EU and the United States diverge significantly in how the governments conceptualize, monitor, and enforce data privacy laws. Due to the significance of international flows of personal information between the two continents, reaching over $260 billion in annual digital services trade,[56] the stakes are high when it comes to data privacy law. The United States views the EU's efforts to protect their citizens' privacy rights against U.S. companies like Google and Facebook with skepticism, and questions whether they are merely disguised protectionism.[57] On the other hand, the EU has long debated whether U.S. law provides sufficient protections for the data privacy rights of EU citizens when U.S. companies and public authorities collect and process it.[58] The struggle between EU regulatory authorities and U.S. corporations over data privacy standards is a "part of a pattern of transatlantic data privacy tensions."[59] Europe has been successful in setting global legislative standards in privacy, but U.S. corporations have set the default standards for processing data on Internet users.[60]

The EU model places comprehensive legislative limits on data privacy rights because they are recognized as fundamental rights pertaining to data protection. This language of rights creates a connection between data subjects and the EU institutions that safeguard these interests.[61] A discussion on rights forms a critical part of the postwar European project of creating the identity of a European citizen, which is a constitutional task "central to the EU's survival."[62] Furthermore, the EU

55. FEILER, *supra* note 9, at 15–16.

56. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 117 (2017) (citing Penny Pritzker & Andrus Ansip, *Making a Difference to the World's Digital Economy: The Transatlantic Partnership*, TRADOLOGY (Mar. 11, 2016), https://blog.trade.gov/2016/03/11/making-a-difference-to-the-worlds-digital-economy-the-transatlantic-partnership/ [https://perma.cc/AQY7-NMWL]).

57. Schwartz & Peifer, *supra* note 56, at 118.

58. *Id. See generally* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995).

59. BYGRAVE, *supra* note 40, at 119.

60. *Id.*

61. Schwartz & Peifer, *supra* note 56, at 121.

62. *Id.* at 119.

has a collective approach to ordering privacy. Therefore, the EU limits contract and consent through strict requirements of necessity and purpose limitation.

In the United States, data privacy law is based on the idea that consumers merit governmental protection in a marketplace marked by deception and unfairness. The focus is on "marketplace discourse" about personal information and the safeguarding of privacy consumers.[63] U.S. legislation permits a significant degree of contractual "override" of data privacy rights because data privacy is not a constitutionally protected right.[64] The primary constitutional safeguards for information in the United States concern the free flow of data under principles of free speech pursuant to the First Amendment, not personal privacy. In the absence of a comprehensive legislative framework, the individual resort to data privacy in the United States has "at best, a contractual footing."[65] Moreover, U.S. privacy regulations target specific, sectorial activities. As a result, some businesses in the United States have collected and used personal data without consumers' knowing consent or contract, as long as they followed certain sector laws, state laws, or other mandates not to harm consumers through deception and unfair practices.[66]

But even within the United States, distinctions do exist between the general U.S. legislative approach to data privacy law and California's state laws regarding privacy. The next Section discusses in detail the EU model and the laws behind the development of data privacy laws in the EU and the resulting GDPR. The Section immediately following the next one focuses on California's data privacy regulatory approach and the data privacy concerns behind the enactment of the CCPA.

1. The EU Model and the GDPR

In 1995, the European Union adopted the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, also known as the EU Data Protection Directive (1995 Directive).[67] The 1995 Directive was founded upon a fundamental right to respect private life and the protection of personal data guaranteed by Articles 7 and 8 of the European Charter, passed in 2000.[68] It also adhered to Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), providing that the protection of natural persons in relation to the processing of personal data is a fundamental right.[69] The term "data protection" widely used in the EU in reference to data

63. *Id.* at 120.

64. BYGRAVE, *supra* note 40, at 118.

65. *Id.* at 118–19.

66. Schwartz & Peifer, *supra* note 56, at 120.

67. *See* Directive 95/46/EC, of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 25, 1995 O.J. (L 281) [hereinafter Directive 95/46/EC].

68. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1 [hereinafter Charter].

69. Treaty on the Functioning of the European Union, art. 16, Dec. 13, 2007, 2012 O.J. (C 326) 1.

privacy rights of European citizens directly correlates with the phrase "protection of personal data" articulated in the European Charter, TFEU, and the 1995 Directive.

The initial data protection regime provided by the 1995 Directive sought to harmonize the protection of fundamental rights of data privacy and the transfer of personal data to third countries outside the Union. The 1995 Directive conditioned data transfers only to countries authorized as having adequate levels of protection for data comparable to the protections within the EU.[70] However, European lawmakers became aware of deficiencies in the 1995 Directive because it left some room for interpretation among individual states and was not audited. Moreover, the rapidly changing landscape in data storage, collection, and transfer necessitated an update to the EU's regulatory environment.

Compounding these factors, revelations that the U.S. intelligence community conducted mass surveillance of foreign citizens through PRISM came to light in 2013. A subsequent but unrelated determination by the European Court of Justice in the 2015 *Schrems v. Data Protection Commissioner* case made it clear that the 1995 Directive was inadequate in practice.[71] The *Schrems* court invalidated the Decision 2000/520 EU-US safe harbor laws under which American companies could self-certify in order to engage in cross-border data transfers between Europe and the United States, giving way to a replacement law.[72] The EU-US Privacy Shield was hastily agreed upon within the span of one year to allow over 5,000 U.S. companies to continue doing business with the EU states, and safely process and transfer personal data of EU citizens under a safe harbor law for the next two years until the GDPR came into effect. Where the Privacy Shield was seen as weak and unable to prevent U.S. intelligence activities on EU citizens,[73] the GDPR was set to allay European concern about how U.S. companies handle private data. Under the GDPR, U.S. companies were expected to fully comply with much more restrictive privacy laws or face steep fines.

The European Commission replaced the 1995 Directive with the GDPR, effective May 25, 2018.[74] The Commission initially proposed an update to the

---

70. Directive 95/46/EC, *supra* note 67.

71. *See* Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 E.C.R. I-35 ¶¶ 98–103.

72. *Schrems v. Data Protection Commissioner*, GLOBAL FREEDOM OF EXPRESSION COLUM. U., https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/ [https://perma.cc/E557-MQ6E] (last visited Nov. 12, 2019).

73. Jamie Carter, *How to Handle the New US-EU Data Regulations*, TECHRADAR (May 23, 2016), https://www.techradar.com/news/internet/how-to-handle-the-new-us-eu-data-regulations-1320554 [https://perma.cc/P37J-F35P]; *Max Schrems v. Data Protection Commissioner*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/intl/schrems/ [https://perma.cc/L6J4-AUCN] (last visited Nov. 12, 2019).

74. 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), 2016 O.J. (L 119) [hereinafter GDPR].

existing data protection regulation "to make Europe 'fit for the digital age'" in January 2012.[75] Approved on April 14, 2016, the GDPR aimed to strengthen, unify, and make more coherent data protection laws and its framework across the twenty-seven EU member states.[76] The Commission sought to correct the distortion of competition between states due to unequal data protection laws and fortify monitoring and enforcement to bring more companies and organizations into compliance with EU laws.[77] Once the GDPR entered into force, the original 1995 Directive was repealed and all laws brought into conformity with the new data privacy regulation.[78] Unlike the 1995 Directive, the GDPR was a digital "single market strategy" that was automatically applicable to all EU member states without the need for implementing national legislation in each EU member state.[79]

The GDPR expands upon earlier legal standards such as the 1995 Directive, the European Charter, TEFU, and the Privacy Shield in crucial ways. The GDPR was founded upon important principles of transparency, lawfulness, fairness, data minimization, right to be forgotten and right to erasure, and subject to considerations of necessity and purpose.[80] Accordingly, the GDPR diverges from prior legislation in various ways. First, the GDPR sets a higher bar for obtaining personal data than had been allowed before by requiring explicit and informed consent from users. Second, it seeks to simplify and extend the reach of the regulatory environment for businesses that are controllers and processors so both citizens and businesses in the EU can fully benefit from the digital economy. Third, the penalties are severe enough to ensure companies and organizations comply with the new measures. Fourth, the rights of data subjects are expanded to give EU citizens more user control over their personal data. Lastly, the GDPR sets a hard deadline for companies: the new rules went into effect on May 25, 2018. In other words, if a company failed to follow the rules by then, it would run into trouble. This has resulted in companies scrambling to adapt their policies to the new rules,

---

75. Danny Palmer, *What Is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 17, 2019, 6:33 PM), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/ [https://perma.cc/X5R3-3X57].

76. GDPR, *supra* note 74, ¶¶ 7, 9, 10.

77. *Id.* ¶ 9.

78. *Id.* ¶ 171, at 31.

79. *See The Single Market Strategy*, EUR. COMMISSION, http://ec.europa.eu/growth/single-market/strategy_en [https://perma.cc/YV4G-ZWRD] (last visited Nov. 12, 2019).

80. *See* GDPR, *supra* note 74, art. 5, § 1(a)-(f) ("Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes . . . ; (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; . . . ensur[ing] that personal data that are inaccurate, . . . are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary . . . ; [except for] data . . . processed solely for archiving purposes in the public interest, scientific or historical research or statistical purposes . . . ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data . . . ('integrity and confidentiality')").

pulling users out of reach of EU privacy laws[81] or blocking EU citizens' access to online services like newspapers[82] in order to avoid the steep penalties.

The GDPR upholds the rights of EU data subjects to a strict standard. As a body of law, the GDPR integrates the most recent technological developments and the challenges that have brought the protection of personal data to the forefront of public debate in the EU and the United States. It follows the trend of increased public concern over privacy. The GDPR guarantees the rights of data subjects over significant areas, such as breach notification, right to access information, right to erasure (to be forgotten), data portability, and privacy by design and by default. This Note solely focuses on informed consent and the right to be forgotten.

2. The California Model and the CCPA

A right of privacy is not directly expressed in the U.S. Constitution or the Bill of Rights. Nevertheless, the U.S. Supreme Court has held that privacy is implicitly protected by the Equal Protection Clause of the Fourteenth Amendment to the U.S. Constitution.[83] In 1972, California made a radical departure and passed a constitutional provision recognizing the "inalienable" right to privacy[84] that applies to both government and private actors.[85] At the California Legislature's urging, the people of California voted to amend the California Constitution through an initiative process to include the rights of privacy among the rights of all people.[86] The ballot argument for the initiative observed that the California constitutional right of privacy "prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us."[87] In subsequent rulings related to privacy rights of California residents, California high

81. Alex Hern, *Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law*, GUARDIAN (Apr. 19, 2018), https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law [https://perma.cc/B6Z9-A2ZH].

82. Bloomberg, *Blocking 500 Million Users Is Easier than Complying with GDPR*, FORTUNE (May 25, 2018, 7:03 AM), http://fortune.com/2018/05/25/gdpr-compliance-lawsuits/ [https://web.archive.org/web/20200516003030/https://fortune.com/2018/05/25/gdpr-compliance-lawsuits/].

83. *See generally* Lawrence v. Texas, 539 U.S. 558, 564–65 (2003); Roe v. Wade, 410 U.S. 113, 152–53 (1973); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972); Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

84. CAL. SEC'Y OF STATE, VOTER INFORMATION GUIDE FOR 1972, GENERAL ELECTION 26 (1972).

85. Section 1 of the California State Constitution states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. 1, §1; *see also* Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797, 808 (Cal. 1997).

86. The privacy amendment was originally proposed by Representative Kenneth Cory in 1972 as Assembly Constitutional Amendment 51. The legislative initiative was placed upon the November 1972 ballot and was approved by the people. Article 1, Section 1 was subsequently amended. *See also* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 328 (1992).

87. CAL. SEC'Y OF STATE, *supra* note 84, at 27.

courts have indicated that the scope of the protection granted by the state constitution's explicitly enumerated privacy right is sometimes greater than the scope of the U.S. Constitution's unenumerated right of privacy.[88]

White v. Davis was the first California Supreme Court case to interpret the Privacy Amendment, solidifying the constitutional rights to informational privacy by explaining the need for privacy protections:

> [T]he moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision's primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy.[89]

In 1994, *Hill v. National Collegiate Athletic Association* laid out the analytical framework, determining that a constitutional violation of privacy interests must set forth threshold elements: (1) a legally protected privacy interest, (2) a reasonable expectation of privacy in the circumstances, and (3) conduct by defendant constituting a serious invasion of privacy.[90] The first element is typically of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential info and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference.[91] The first class touches upon informational privacy, a core value recognized as the "need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity."[92] The second essential element constitutes a reasonable expectation of privacy, looking at the customs, practices, and physical setting, as well as whether there was advance notice of the intrusion and whether there was voluntary consent to activities affecting privacy interests.[93] The privacy invasion must be sufficiently serious in nature, scope, and impact to constitute an egregious breach of social norms, balanced against competing interests such as governmental activities or private entities.[94] Yet, the identified privacy intrusion must be balanced against competing interests, which may be justified if legitimate interests derived from legally authorized and socially beneficial activities of the government and private entities.[95] A plaintiff may rebut a defense based on countervailing interests with a showing of alternative measures to the defendant's

88. *See* Comm. to Defend Reprod. Rights v. Myers, 625 P.2d. 779 (Cal. 1981); City of Santa Barbara v. Adamson, 610 P.2d 436, 446 n.3 (Cal. 1980) (noting that the federal right to privacy "appears to be narrower than what the voters approved in 1972 when they added 'privacy' to the California Constitution.").

89. White v. Davis, 533 P.2d 222, 233 (Cal. 1975).

90. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 656–57 (Cal. 1994).

91. *Id.* at 654.

92. *Id.*

93. *Id.* at 655–56.

94. *Id.*

95. *Id.*

conduct that would have minimized the invasion of privacy interests.[96] The specific kind of privacy interest involved, the nature and seriousness of the invasion, and any countervailing interests constitute critical factors in the analysis.[97] This analysis has been linked to online privacy and tracking using cookies.[98]

Furthermore, the judicial balancing may differ if it is a government entity or private actor.[99] The right to privacy may not apply as stringently to private actors, the California Supreme Court noted. Government intrusion into privacy typically has the capacity to be far more detrimental to personal privacy than an intrusion by a private entity because the government has more power and resources available to it than a private entity.[100] The Court stated that an individual has greater choice in dealing with private actors than when dealing with the government.[101] Although if a "private entity controls access to a vitally necessary item," it may tip the balance toward the plaintiff.[102] Nevertheless, corporations should still be concerned because the law applies to a corporation's interactions with California customers and employees, and may be "especially vulnerable under the realm of information privacy."[103]

Similar to other states, California common law has traditionally protected against invasions by private actors through tort actions. The four common law privacy torts are (1) intrusion into a person's solitude or seclusion, (2) publicity that puts a person in a false light, (3) public disclosure of embarrassing private facts, and (4) commercial appropriation of a person's name or likeness.[104] The common law action for invasion of privacy protected somewhat well-defined aspects of personal privacy, but privacy was not accorded a "privileged place or undue weight in the balancing process."[105] Courts "did not attempt to define 'privacy' itself," rather carving out "particular aspects of privacy . . . deserving protection," until the privacy clause was enacted.[106]

California has long since cemented its reputation as a strong proponent of data privacy laws by enacting a series of laws protecting consumers' data privacy rights. In 2002, California passed Senate Bill 1386, or section 1798.29 of the California Civil Code, the first bill of its kind requiring breach notification to consumers.[107]

---

96. *Id.* at 656.

97. *See* Sheehan v. San Francisco 49ers, Ltd., 201 P.3d 472, 477 (Cal. 2009) (citing *Hill*, 7 Cal. 4th at 34).

98. *See In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

99. *Hill*, 865 P.2d at 656.

100. *Id.*

101. *Id.*

102. *Id.* at 657.

103. Margaret Betzel, *Privacy Law Developments in California*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 831, 837 (2006).

104. *See* Hernandez v. Hillsides, 211 P.3d 1063, 1072–73 (2009); Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 478 n.4 (1998).

105. Kelso, *supra* note 86, at 376.

106. *Id.* at 386.

107. CAL. CIV. CODE § 1798.29 (West 2012).

The bill requires any businesses doing business in California and owning computerized data of California residents to provide prompt notice to California consumers "of any breach of security involving unencrypted personal data."[108] Every state in America has enacted similar laws since then.[109]

A series of other laws directed at protecting electronic consumer data collected and maintained by businesses have been passed. The Online Privacy Protection Act (Cal-OPPA) enacted in 2004 is a major law targeting operators of commercial websites and online services that collect personal information online to post privacy policies on their website.[110] Consumer Protection Against Computer Spyware Act of 2004 prohibits nonauthorized users from knowingly or willfully installing spyware into a user's computer.[111] California's data breach laws codified in sections 1798.29 and 1798.80 *et seq.* of the California Civil Code require businesses to take reasonable steps to destroy customer records that contain personal information once the company finishes using them.[112] Assembly Bill 1950 requires businesses that own or license personal information to implement security safeguards against unauthorized access.[113] Recent laws include AB 370, which amended Cal-OPPA in 2014, to require disclosure in privacy policies of how companies' websites respond to behavioral tracking or Do Not Track (DNT) browser settings selected by online users.[114] The amendment addresses concerns that companies need to provide more "comprehensive privacy policy disclosures . . . to the public" in regards "to the full range of businesses' data privacy and security practices."[115] Another revision to Cal-OPPA includes the "Privacy Rights for California Minors in the Digital World" chapter, effective January 1, 2015, allowing minors to erase information online.[116] The bill imposes obligations on any website, application, or other online service that

108. Betzel, *supra* note 103, at 855; *see* CIV. § 1798.29(a).

109. FEILER, *supra* note 9, at 328; *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://web.archive.org/web/20181008001850/https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx].

110. Lydia F de la Torre, *What Is 'CalOPPA'?*, MEDIUM (May 11, 2019), https://medium.com/golden-data/what-is-caloppa-b781b0cd5e39 [https://perma.cc/ZA85-3X3V].

111. *California Goes After Spyware*, WIRED (Oct. 2, 2004, 7:17 AM), https://www.wired.com/2004/10/california-goes-after-spyware/ [https://perma.cc/ULR5-WQWW].

112. *Data Breach Notification Law in California*, SECURITY COMPLIANCE ASSOCIATES (Nov. 22, 2019), https://www.scasecurity.com/data-breach-notification-law-in-california/ [https://perma.cc/KE7U-KW5U].

113. Jonathan P. Armstrong & Bruce A. Heiman, *Data Breach Notification and Cybersecurity Standards in the U.S. and E.U.*, BNA INT'L'S WORLD INTERNET L. RPT., Dec. 2005, http://www.klgates.com/files/Publication/450eb4c8-af93-4ec9-80c0-16de7a34f570/Presentation/PublicationAttachment/715df338-f7d0-404b-be86-23d14b429b68/BNA_heiman.pdf [https://perma.cc/USU5-2GAQ].

114. Dominique Shelton & Paul Martino, *California AG Kamala Harris Issues Privacy Policy Guidance; Contains Draft Tips for Website and Online Service Privacy Policies*, 19 CYBERSPACE LAW. 1, 3 (2014).

115. *Id.* at 4.

116. CAL. BUS. & PROF. CODE § 22581(a)(1) (West 2014); *id.* § 22582.

(1) is directed to minors— "an audience predominantly composed of minors"—or (2) has actual knowledge that a minor is using it.[117] Significantly, this law requires a Covered Service to permit a registered user under eighteen to (a) remove content that he or she has posted to the service and (b) provide instructions (e.g., in the privacy policy) on how to request removal of posted content.[118] Other enforcements have aimed to protect consumers from data breaches, for which more than 1.4 million Californians were at risk in 2013, and places myriad of companies at risk of facing private lawsuits.[119]

On June 28, 2018, California legislature passed the California Consumer Privacy Act of 2018 (CCPA), also known as Assembly Bill 375.[120] The bill was the result of a last-minute compromise between state Democrats and privacy advocates without opposition.[121] The bill was signed "just hours before a deadline to pull from the November ballot an initiative seeking even tougher oversight over technology companies."[122] AB 375 garnered more than 600,000 signatures from Californians in the face of heavy lobbying from tech companies who spent millions of dollars to oppose it.[123] Heavily supported by California consumer advocates, the CCPA grants consumers a number of data privacy rights that includes the right to request businesses to delete any personal information they may have, the right to request businesses that sell personal information to disclose categories of information sold and to identify third parties to which it was sold, and the right of consumers to opt out of the sale of their personal information.[124]

Entities doing businesses in California are covered by the bill if they meet specific requirements such as an annual gross revenue over twenty-five million dollars, for businesses that buy, sell, or share for commerce the personal information of more than 50,000 consumers, households, or devices; or derives fifty percent or more of their annual revenues from selling consumers' personal information.[125] The compromise reached before the passage of the bill limited legal damages and provided significant concessions to business opponents. The concessions have warranted that private consumer action is actionable, but

---

117. *Id.* § 22580(e) (2019); *id.* § 22581(a) (2014).

118. *Id.* § 22581(a)(1)–(3).

119. Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under the FTC Act and California Unfair Competition Law*, 32 COMPUTER & INTERNET LAW. 14, 19 (2015).

120. Assemb. B. 375, 2017-2018, Reg. Sess., § 1798.1000 (Cal. 2018) [hereinafter A.B. 375].

121. Colin Lecher, *California Just Passed One of the Toughest Data Privacy Laws in the Country*, VERGE (June 28, 2018, 3:46 PM), https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote [https://web.archive.org/web/20200417033223/https://www.theverge.com/2018/6/28/17509720/california-consumer-privacy-act-legislation-law-vote].

122. Wakabayashi, *supra* note 1.

123. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/ [https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/].

124. *Id.*; Noah Ramirez, *Can CCPA Affect Your Small Business?*, OSANO (Oct. 30, 2019), https://www.osano.com/articles/ccpa-small-business [https://perma.cc/4KCC-6FT7].

125. A.B. 375, § 1798.140(c)(1)(A)–(B).

businesses must be provided with a thirty-day written notice to "cure" any alleged violations before an action is undertaken.[126] Moreover, the bill "leaves the task of enforcing the law to the attorney general and takes the right to private action by citizens off the table, except in the case of data breaches," in view of tech companies' arguments that the CCPA "opens them up to liability that would hurt their businesses and their ability to hire."[127]

Riding on the back of the GDPR wave bolstering consumer advocacy for data privacy rights, the passage of the CCPA is no doubt part of a growing trend towards increased data protection for consumers. The GDPR is broader than the CCPA in many aspects, but significant overlaps exist in the legal boundaries for protecting consumers and businesses' corresponding obligations. Whether there are factors that distinguish the CCPA from the GDPR will be examined in closer detail looking at two specific provisions: (1) the opt-in vs. opt-out consent and (2) the right to be forgotten. The following Section will conduct a comparative study to determine the principles that drive the regulations.

II. COMPARATIVE STUDY OF THE GDPR AND THE CCPA

A. Opt-In vs. Opt-Out Consent

Opt-in and opt-out consent are concepts in the field of data processing rooted in contractual principles.[128] Data processing on the Internet creates a relationship between a business and the Internet consumer who engages in activities on the program or platform maintained by an online data processor such as a social media website and other online websites. This means that people have become the product[129] because data processing plays an important role in online behavioral advertising.[130] Online data processing and behavioral advertising now relies on collection of huge amounts of data from countless "number[s] of actors engaged in commercial activities online," mostly without the consent of individuals whose data is being processed.[131] Individuals do not have much "choice in being commodified for firms' financial gain or preventing the privacy invasions that profiling entails," but the practice itself can harm individuals' dignity and autonomy.[132]

The opt-in regime is the act of requiring online commercial actors to receive an individual's "express, affirmative and informed consent before engaging in data

126. *Id.* § 1798.150(b).

127. Lapowsky, *supra* note 123.

128. Nicklas Lundblad & Betsy Masiello, *Opt-In Dystopias*, 7 SCRIPTED 155, 160 (2010).

129. Julia Angwin, *Has Privacy Become a Luxury Good?*, N.Y. TIMES, Mar. 4, 2014, at A23 ("[I]f you aren't paying for the product, you are the product.").

130. Joseph A. Tomain, *Online Privacy and the First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 3 (2014).

131. *Id.* (citing Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000)).

132. Tomain, *supra* note 130, at 3–4.

processing."[133] This requirement compels online commercial actors to consider and weigh in on "individual privacy, autonomy, dignity, and democratic participation interests" balanced against the financial interests of private businesses.[134] "In the strictest interpretation, opt-in consent . . . impl[ies] that a user has affirmatively agreed to the disclosure and use of his information in every instance."[135] A loose interpretation of opt-in consent holds that "a single click . . . implies consent on behalf of all users of a particular browser."[136]

However, "a common criticism of opt-in is that it imposes excessive costs on the user."[137] In the context of a cookie-based information collection, imposing a "loosely interpreted opt-in process would presumably require that at every *initial* interaction with a site where a cookie is set, the user is asked for consent to collect information about his or her behavior on that site."[138] After this initial consent, the website would subsequently remember the preference "so that in future visits the consent is remembered."[139] As a result, it is generally accepted that "cookie-based information collection is often understood to be opt-out: a user can decline cookies or reset them but the typical default action of most browsers is to accept cookies and enable this information collection."[140] To circumvent the costs of requesting preferences during each interaction, many sites require user registration in order to remember their preferences, which "can be used to gain a one-time, loose but persistent opt-in consent to information collection and use, at low cost to the user, and theoretically with the user's affirmative consent."[141]

The opt-out rule "plac[es] the burden on the individual to prevent certain types of information from being shared," and thus "promotes the free-flow of information."[142] The current default for websites doing business in the United States is that "an individual has to opt-out of data processing, if there is such an option at all."[143] The opt-out regime can occur "[w]hen an individual downloads an app" (e.g., Pokémon Go) and the user "automatically consents to the access of her personal information without receiving a notification to allow such access."[144] Typical language as evidenced by the Privacy Policy in Pokémon Go states, "[y]ou understand and agree that by using our App you (or your authorized child) will be transmitting your (or your authorized child's) device location to us and some of that

133. *Id.* at 4.
134. *Id.*
135. Lundblad & Maisello, *supra* note 128, at 158.
136. *Id.*
137. *Id.* at 159.
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.*
142. Julia Palermo, Comment, *You Say "Tomato," I Say "Tomahto:" Getting Past the Opt-In v. Opt-Out Consent Debate Between the European Union and United States*, 9 GEO. MASON J. INT'L COM. L. 121, 121 (2017).
143. Tomain, *supra* note 130, at 12.
144. Palermo, *supra* note 142, at 121.

location information, along with your (or your authorized child's) user name, may be shared through the App."[145] The user may rescind consent by submitting an email to the game creator but if certain information cannot be shared, the user may not be able to use all features of the game.[146]

The major criticism against the opt-out regime is that "an opt-out mechanism is insufficient due to informational asymmetry and power imbalances between individuals and private commercial actors, as well the natural financial incentive of firms to maintain these conditions."[147] The default opt-out regime results in privacy policies that are notoriously vague and broad, making it difficult for consumers to have meaningful notice and consent, because "firm[s] [have] natural business incentives to prevent the individual from opting out."[148] "From a financial perspective, the failure to disclose data processing practices or offer the ability to opt-out . . . is strategically sound."[149] In fact, companies have every incentive to keep these transaction costs high in order to discourage consumers from taking steps to avoid data collection.[150] "When consumers exercise the option of having their names deleted," the customer "lists shrink and become less valuable" and companies incur transaction costs in responding to consumers who opt out.[151] As a result, companies that "offer opt-outs have an incentive to increase the transaction costs incurred by consumers who opt out" by making it difficult for users to opt-out by providing ineffective privacy notices that are difficult to read.[152]

Yet, the problem with businesses providing privacy notices that are lengthy, hidden, small-printed, and written in legalese is a problem that applies to both opt-in and opt-out regimes. "Many existing policies are long, complex, confusing, and self-contradictory."[153] Not to mention, "privacy policies often go unread."[154] Consumer indifference to privacy concerns cannot be counted out; but to make matters worse, one study found that, "it would take an average of 201 hours per year for an individual to read the privacy policies of all the websites she visited in a

145. *Pokémon GO Privacy Policy*, NIANTIC, https://www.nianticlabs.com/privacy/pokemongo/en/ [https://web.archive.org/web/20161223070144/https://www.nianticlabs.com/privacy/pokemongo/en/] (last updated Dec. 21, 2016).

146. *Id.*

147. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2 (2014) ("While big data will be a powerful engine for economic growth and innovation, there remains the potential for a disquieting asymmetry between consumers and the companies that control information about them."); Tomain, *supra* note 130, at 16–17.

148. Tomain, *supra* note 130, at 12.

149. *Id.* at 23.

150. Jeff Sovern, *Opting in, Opting out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1081–82 (1999).

151. *Id.* at 1082.

152. *Id.* at 1083–87.

153. Malla Pollack, *Opt-In Government: Using the Internet to Empower Choice—Privacy Application*, 50 CATH. U. L. REV. 653, 675 (2001).

154. Tomain, *supra* note 130, at 13.

year."[155] This shows that even privacy-conscious consumers may act inconsistent with regard to their preferences because (1) they cannot find the time to "manage effectively consumption that has grown more complex and dynamic," and (2) consumers' interests are "spread thinly across thousands of transactions and the management of hundreds of possessions," meaning that "amateur-generalists" must deal with experts in the field.[156]

But the growing consensus, especially in the era of massive data breaches and privacy intrusions, is that the opt-in model better protects consumers over opt-out model because the opt-out model promotes a form of self-regulation for online business that does not work: businesses require a strong governmental push.[157] To note, the Federal Trade Commission has long taken the position that the opt-in model is the preferred method for protecting consumer interests because it provides informed consent.[158] Yet, determining "what is set as a default setting can often make more difference than the options that are actually offered" from the perspective of an Internet user.[159] Accordingly, the opt-in model and the informed consent required through pop-up windows would theoretically better protect the user's privacy.

1. Application

Although the GDPR does not explicitly use the term "opt-in," its definition of consent coupled with the conditions for valid consent show that it requires opt-in consent before data processing may occur. Informed consent is a cardinal element of the GDPR. The GDPR defines consent as "a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her."[160] Further, affirmative consent provides that "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent."[161] In other words, an opt-out approach is not sufficient.

The GDPR has removed any possibility of opt-out consent in its other provisions. For example, consent is not freely given if there is "a clear imbalance

---

155. *Id.* (quoting Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 562 (2008) ("Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually.")).

156. Sovern, *supra* note 150, at 1091.

157. Pollack, *supra* note 153, at 654 (referencing a Federal Trade Commission report that "the self-regulating motion picture, music recording, and electronic game industries routinely target children 17 as the audience . . . that the industries themselves acknowledge are inappropriate for children"); *see FTC Releases Report on the Marketing of Violent Entertainment to Children*, FED. TRADE COMMISSION (2000), http://www.ftc.gov/opa/2000/09/youthviol.htm [https://perma.cc/NUB6-LT9C].

158. *See* Tomain, *supra* note 130, at 27–31.

159. PAUL BERNAL, INTERNET PRIVACY RIGHTS: RIGHTS TO PROTECT AUTONOMY 38 (2014).

160. GDPR, *supra* note 74, ¶ 32.

161. *Id.* ¶ 32.

between the data subject and the controller, in particular where the controller is a public authority."[162] Moreover, the data controller must be able to demonstrate that the data subject has consented to the processing of personal data through a written agreement "clearly distinguishable from the other matters" and presented it in an "intelligible and easily accessible form."[163] This requirement is intended to avoid the problem of data controllers hiding important terms regarding data processing from other contractual terms. Furthermore, a data subject must be free to withdraw consent at any time as easily as it was to give consent.[164] The presumption is that consent is not freely given "if it does not allow separate consent to be given to different personal data processing operations."[165] This provision allows consent to be purpose-limited to the extent that the consent automatically loses validity once the purpose is fulfilled with one provider or the use of the data is no longer necessary for that purpose.[166] Accordingly, each provision under the GDPR's opt-in regime creates a higher burden for controllers to meet the GDPR standard when asking data subjects for consent to process data. The default opt-in requirement under the GDPR evinces a concern to bolster user control over one's personal data by disallowing companies from using data outside of the scope under which a user gave consent. Requiring companies to adopt opt-in measures changes the paradigm so that companies are under stringent standards to abide by new regulations and rein in ways that companies may have misused personal data for their own profit-generating purposes.

In contrast, the CCPA veers away from the GDPR opt-in regime by providing an opt-out regime. Under section 1798.120(a), the CCPA gives consumers the right to "opt out" of a business selling their personal information to third parties.[167] The bill provides a very broad definition of information sold by businesses, because "personal information" is inclusive of "a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information."[168] Businesses must provide notice that information collected may be sold and that consumers have the right to opt out of the sale of their personal information.[169] Moreover, a business must comply with the opt-out provision by providing a "clear and conspicuous link on the business' Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information."[170] As such, businesses will likely have to create a separate

162. *Id.* ¶ 43.
163. *Id.* art. 7, at 1–2.
164. *Id.* art. 7, at 3.
165. *Id.* ¶ 43.
166. Tomain, *supra* note 130, at 35.
167. A.B. 375, 2017-2018, Reg. Sess., § 1798.120(a) (Cal. 2018).
168. *Id.* at Preamble.
169. *Id.* § 1798.120(b).
170. *Id.* § 1798.135(a)(1).

contact form dedicated to processing visitor requests to opt out of data collection.[171] There must also be a link provided to the "Do Not Sell My Personal Information" page in a business' online privacy policy or any California-specific description of consumers' privacy rights.[172] After receiving a consumer's opt-out request, the business must refrain from selling personal information collected by the business for at least twelve months before contacting the consumer again seeking authorization on the sale of the consumer's personal information.[173]

At first look, the opt-out model in the CCPA gives consumers a more visible choice not to agree to data collection compared to the current situation. The CCPA also emphasizes the importance of receiving the consumer's consent before engaging in the business practice of selling the consumers' personal information to third parties. Accordingly, the current draft of the CCPA is a valid attempt to correct the informational asymmetry and power imbalances between individuals and private commercial actors, as well the natural financial incentive of firms to maintain these conditions, by requiring businesses to provide a more visible notice and obtain meaningful consent from consumers. Knowing that businesses try to discourage consumers from taking steps to avoid data collection, the CCPA has raised the compliance standard for businesses to more proactively address and rectify consumers' privacy concerns.

At the same time, CCPA's opt-out provision is not on par with the opt-in model followed by the GDPR. Under an opt-in regime, informed consent for each data subject requires the user to affirmatively consent to data collection on a pop-up window or something similar every time the user accesses a website.[174] However, the opt-out model under the CCPA provides a narrower set of rights for a consumer based in California, who is by default consenting to data collection for every website he logs into unless he is actively searching a link to the "Do Not Sell My Personal Information" to sign up to the opt-out contact form list. Interestingly, section 1798.125 of the CCPA allows business to offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of personal information.[175] The financial incentive program should clearly notify consumers and a business may enter into a contract with a consumer, "only if the consumer gives the business prior opt-in consent . . . clearly describ[ing] the material terms of the . . . program, and which may be revoked by the consumer at any time."[176] Accordingly, the only time the CCPA mentions any opt-in consent requirement is in reference to the financial incentive program aforementioned,

171. Dan Goldstein & Adam Rowan, *What Does the California Consumer Privacy Act Mean for IP Attorneys and Law Firms*, 11 A.B.A. SEC. OF INTELL. PROP. LANDSLIDE 22 (2018).

172. A.B. 375, § 1798.135(a)(2).

173. *Id.* § 1798.135(a)(5).

174. Hanna Kozlowska, *Here's Why You Really Shouldn't Ignore That Pop-up from Facebook*, QUARTZ (May 24, 2018), https://qz.com/1288072/facebook-pop-ups-the-social-network-is-rolling-out-its-gdpr-controls-to-users-worldwide/ [https://perma.cc/PC4Y-H4TD].

175. Assemb. B. 375, § 1798.125(b)(1).

176. *Id.* § 1798.125(b)(3).

whereby the consumer must affirmatively consent to the material terms of a business's financial incentive program in order to receive financial compensation in exchange for selling his personal information to the business.

Upon review of the texts in the CCPA and GDPR, it is readily apparent that the opt-out provision in the CCPA does not protect consumers as strongly as the opt-in consent in the GDPR does. In fact, the CCPA allows businesses greater latitude to dictate the terms under which they can provide their Internet services to consumers, as opposed to the GDPR, which can be seen as a sharp rebuke to businesses who until now have profited at the expense of consumers who unwittingly had their personal data collected, retained, experimented with, disclosed, and sold to third parties by Internet businesses over the years.

B. The Right to be Forgotten

In March 2014, the "right to be forgotten" was recognized by the European Court of Justice (ECJ) in the seminal case *Google Spain SL v. AEPD and Costeja Gonzalez*.[177] Simply put, the core provision of the right to be forgotten is that "[i]f an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system."[178] This right extends over personal data that people have given out themselves, and the recognition that this right ultimately puts power in the Internet users to control the data they released online.[179] *Google Spain* in fact acknowledged the right to be forgotten by affirming European Internet users' right to remove or delist weblinks containing their personal information from search engine databases, so that it no longer appears in the search results.[180] Costeja González, a Spanish citizen, brought this lawsuit to prevent Google from providing the public access to an old newspaper article about González that was no longer relevant.[181] The ECJ in *Google Spain* upheld a ruling ordering Google to delete information that was "inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes [for which data were collected or processed]," even if that information is truthful.[182] Since the decision, search engines and other Internet

177. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales, 2014 E.C.R 317.

178. Press Release, Speech of Viviane Reding, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5 (Jan. 22, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF [https://perma.cc/AUB3-9X4P].

179. John Hendel, *Why Journalists Shouldn't Fear Europe's 'Right to Be Forgotten*,*'* ATLANTIC (Jan. 25, 2012), https://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/ [https://perma.cc/Z9Y6-9QHD].

180. *Id.*

181. Vincent West, *The Man Who Sued Google to Be Forgotten*, NEWSWEEK (May 30, 2014, 2:13 PM), https://www.newsweek.com/man-who-sued-google-be-forgotten-252854 [https://perma.cc/B5PW-2WLH].

182. *Google Spain*, 2014 E.C.R at ¶¶ 93–94; Paul J. Watanabe, Note, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111, 1128 (2017).

service intermediaries that handle personal data have been inundated with European user requests to have links connecting to information about them removed from Internet search engines. As of February 2018, Google has received 2.4 million requests in the past three years to have search engine results of users deleted under this rule.[183]

The right to be forgotten is a data privacy right secured by the fair information practices (FIP) that seek to ensure the "accuracy, transparency, and instrumental rationality of data processing."[184] The intellectual roots of this right is found in French law, "which recognizes *le droit à l'oubli*—or the 'right of oblivion'—a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration."[185] In the EU, the right to be forgotten has been codified in the 1995 Directive 95/46/EC, which provides that data subjects can rectify, erase, or block the use of data processed in ways that violate its requirements.[186] Article 8(2) of the European Charter also affirms an individual's fundamental right to data protection and the right to have one's data rectified.[187] Relying on the 1995 Directive and Articles 7 and 8 of the Charter, *Google Spain* required the operator of a search engine to remove links to web pages published lawfully by third parties to recognize the right to be forgotten.[188] As the initial adjudicator, operators of search engines are required to balance countervailing rights and interests, although the ECJ has provided that privacy protection "rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information."[189]

The ECJ's posture in *Google Spain* is not without its critics. The European Committee of the British House of Lords found *Google Spain* "unworkable," stating that "[i]t is wrong in principle" to permit search engines to adjudicate delisting decisions.[190] The Index on Censorship has denounced *Google Spain* as "akin to marching into a library and forcing it to pulp books."[191] According to Professor Robert Post, *Google Spain* misunderstands the nature of privacy rights that should

183. Aliya Ram, *Google Receives 2.4m Requests to Delete Search Results*, IRISH TIMES (Feb. 27, 2018), https://www.irishtimes.com/business/technology/google-receives-2-4m-requests-to-delete-search-results-1.3407979 [https://perma.cc/8FRM-5UUJ].

184. 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, 983 (2018).

185. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012).

186. Directive 95/46/EC, *supra* note 67, art. 12(b).

187. Charter, *supra* note 68, art. 8.

188. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales, 2014 E.C.R 317, ¶¶ 89, 99.

189. *Id.* ¶ 99.

190. EUROPEAN UNION COMM., 2D REPORT, EU DATA PROTECTION LAW: A 'RIGHT TO BE FORGOTTEN?', 2014–15, HL-40, ¶ 56, 62 (UK).

191. Index on Censorship, *Index Blasts EU Court Ruling on "Right to Be Forgotten,"* INDEX (May 13, 2014), https://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten [https://perma.cc/FV7U-6RNV].

apply to the public sphere by dismissing Google as a mere profit-making, data-processing corporation when it should be accorded the same legal status as print media.[192] Insofar as Google is engaged in public communication, Post argues that the press should be controlled by the type of privacy protected in Article 7 of the European Charter, under which "[e]veryone has the right to respect for his or her private and family life, home and communications," and is closer in theory to a "dignitary privacy" view of personal information.[193] Dignitary privacy rights define and enforce the proper bureaucratic handling of data, whereas the data privacy right contained in Article 8 of the Charter define and enforce social norms of respectful expression.[194] Because the right to be forgotten exists in both the instrumental right of data privacy under Article 8 and the communicative right of dignitary privacy under Article 7, Post argues that *Google Spain* is an "ambiguous and opaque decision because it is uncertain whether the CJEU sought to preserve the right of data subjects to control personal information or instead to safeguard the dignity of human beings."[195] Post asserts that *Google Spain* should have expounded on the right to be forgotten as the protection of dignitary privacy, which would have resulted in overcoming the doctrinal challenge that underlies the *Google Spain* decision.[196]

The right to be forgotten has generated quite a controversy as some view it as rewriting or erasing history. Consequently, some instead advocate for the "right to delete," a subtly important but different concept from the right to be forgotten.[197] A right to delete focuses on the right to control data, not about censorship; if properly applied, it does not conflict with freedom of expression.[198] A right to delete "changes the rights being balanced and the duties imposed on others: it is balanced against businesses' 'right' to hold data rather than against individuals' right to remember."[199] It stems from the view that people have the right to remember things but "it is much more questionable whether businesses have a right to hold our personal data."[200] As such, a right to delete shifts the paradigm by requiring holders of data to justify their holding of data—that unless you have a strong reason to hold it, data should not be held.[201] Indeed, the default question in this scenario would ask in what circumstances and what kind of data should people *not* have the right to delete?[202] The added rationale to this shift in paradigm would be that from the perspective of privacy and autonomy, if data does not exist, it cannot be

192. Post, *supra* note 184, at 990.
193. *Id.* at 990–91; Charter, *supra* note 68, art. 7.
194. Post, *supra* note 184, at 991–92.
195. *Id.* at 994.
196. *Id.* at 995.
197. BERNAL, *supra* note 159, at 177.
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.* at 200.
202. *Id.* at 202.

vulnerable.[203] Because the fact of the matter is, looking at the activities of leakers and whistleblowers, from WikiLeaks to the likes of Edward Snowden, that "[d]ata, wherever it is, however it is held and whoever it is held by, is vulnerable."[204]

The presumption in favor of the right to delete should be balanced against countervailing interests, divided into six categories: (1) paternalistic view—that society can override individual interest; (2) the community has interest in keeping data; (3) economic or administrative needs of society require records be kept; (4) archival database is necessary to preserve history; (5) freedom of expression should not be chilled; and (6) law enforcement needs data for security purposes.[205] Of critical importance is that "'supporting your business model' should not be a sufficient reason to deny data deletion," an important justification businesses use to oppose the right to delete.[206]

The U.S. approach to the right to be forgotten largely varies from the European approach, even to the extent that the publication of someone's criminal history is protected by the First Amendment.[207] Upholding freedom of expression as a fundamental concern, the U.S. Supreme Court has held that states cannot pass laws restricting the media from disseminating truthful but embarrassing information—such as the name of a rape victim—as long as the information was legally acquired.[208] But only several years ago, California became the first state to adopt a right to be forgotten law applying only to minors on September 23, 2013, which has gained traction in other states since it was passed.[209] The "Privacy Rights for California Minors in the Digital World" grants California minors the right to "remove or . . . request and obtain removal of, content or information" they posted on an operator's website, application, or online service.[210] This bill was passed in recognition of a general sentiment that teenagers frequently self-reveal before they self-reflect, which may unfairly impact the future of teenagers.[211] This bill has been

---

203. *Id.* at 177.

204. *Id.* at 196.

205. *Id.* at 202–03.

206. *Id.* at 204.

207. Rosen, *supra* note 185, at 88 (citing John Schwartz, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, N.Y. TIMES, Nov. 12, 2009, at A13); *see also Walter Sedlmayr*, WIKIPEDIA, http://en.wikipedia.org/wiki/Walter_Sedlmayr [https://perma.cc/CU93-E6YR] (last visited Feb. 6, 2012)) (discussing two Germans convicted of murdering a famous actor who fought to remove their information from being published on the actor's Wikipedia page, but Wikipedia's right to publish someone's criminal history has been protected under the First Amendment.).

208. Florida Star v. B.J.F., 491 U.S. 524, 541 (1989). In *Garcia v. Google, Inc.*, 786 F.3d 733, 737 (9th Cir. 2015) (en banc), Cindy Lee Garcia sued Google to have a film removed from YouTube after she was cast on the film, *Innocence of Muslims*, which contained an anti-Islam polemic. The video garnered millions of views on YouTube, but unfortunately Garcia's inability to control the final product saw her life threatened. The Ninth Circuit upheld Google's right not to have the video taken down.

209. *State Right to Be Forgotten Policy*, ELEC. PRIVACY INFO. CTR., https://www.epic.org/state-policy/rtbf/ [https://perma.cc/DBU2-CZPN] (last visited Mar. 3, 2020).

210. *See* CAL. BUS. & PROF. CODE § 22581 (West 2014).

211. Caitlin Dewey, *How the 'Right to Be Forgotten' Could Take Over the American Internet, Too*, WASH. POST (Aug. 4, 2015, 7:02 AM), https://www.washingtonpost.com/news/the-intersect/wp/

an instrumental and significant step for the state of California to take the next step to grant the right to be forgotten to a broader audience to a certain degree.

i. Application

One of the most important provisions in the GDPR is the incorporation of the right to be forgotten, which encompasses the right to erasure or rectification of personal data under Articles 16 and 17. Under Article 16, data subjects have the right to request the controller rectify inaccurate personal data concerning him or her within one month.[212] Under Article 17, the right to erasure applies if, for instance, (a) the personal data is no longer necessary to the purposes for which they were collected or processed, (b) data subject withdraws consent on which the processing is based and there is no legal basis for the processing, (c) the user objects to the processing and there is no overriding legitimate grounds for the processing of data, and (d) personal data was unlawfully processed.[213] Additionally, the controller has a duty to communicate the user's rectification or erasure of personal data request to each recipient whom the personal data have been disclosed.[214] If the data subject makes a request, the controller should inform the data subject about each of those data recipients.[215]

For personal data made public and for which the controller is obligated to erase the personal data due to duties imposed on it, the controller may request other third party controllers to erase the links or copies or replications of those personal data, taking account of technology and costs involved.[216] This provision addresses the concern that "[t]o strengthen the right to be forgotten in the online environment, the right to erasure should also be extended" to controllers like Google, who must relinquish their right to process the data by erasing them.[217] It is an appropriate measure pursuant to the holding in *Google Spain*.[218] Accordingly, the GDPR reinforces the right to be forgotten as a fundamental principle by detailing, expanding, and defining the scope of the right within its legal provisions. The right to be forgotten comes with important exceptions, such as the right of freedom of expression and information, compliance with other obligations under the EU or member state laws, for reasons of public interest and public concerns, for archiving purposes, and the exercise and establishment of law enforcement and legal claims.[219]

2015/08/04/how-the-right-to-be-forgotten-could-take-over-the-american-internet-too/?noredirect=on&utm_term=.84290d2bde40 [https://perma.cc/HM9Q-4H5D].

212. GDPR, *supra* note 74, art. 16; *Id.* ¶ 59.

213. *Id.* art. 17, at 1.

214. *Id.* art. 19.

215. *Id.*

216. *Id.* art. 17, at 2.

217. *Id.* ¶ 66.

218. *See generally* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales, 2014 E.C.R 317.

219. GDPR, *supra* note 74, art. 16; *id.* ¶ 65.

The CCPA diverges from the GDPR when it comes to the principle of the right to be forgotten. First of all, there is no reference to a right to be forgotten. Instead, the CCPA refers to the "right to delete" under section 1798.105, granting consumers the right to request that "a business delete any personal information . . . which the business has collected from the consumer."[220] Upon receipt of a verifiable request, the business must delete the consumer's personal information from its records and also "direct any service providers to delete [the information] from their records."[221] The disclosure of this rule must be provided to all consumers in the business's online privacy policy or on its website.[222] Exceptions to the rule do exist, which consist of (a) the fulfillment of a contract with the consumer; (b) data security; (c) repair errors; (d) scientific and statistical research in public interest; (e) solely internal uses reasonably aligned with expectation of consumers; (f) compliance with legal obligations; and (g) other internal uses of consumers' personal information in a lawful manner.[223]

Applying a textual analysis approach, it appears that the CCPA's right to delete provision diverges in principle from the right to be forgotten provision under the GDPR. The GDPR faithfully accords with the judgment in *Google Spain* that Internet service providers must delete information that is inadequate, irrelevant, no longer relevant, or excessively outside the purposes for which data were collected or processed.[224] The GDPR also grants the right to erasure or to rectify information that was already guaranteed under the 1995 Directive.[225] In contrast, the CCPA's right to delete conforms to the less controversial and narrower interpretation of an individual's right of control over one's data vis-à-vis the business who seeks to retain the data. The right to delete is much more compatible with the United States' approach to data privacy, where social expectation and protection of the First Amendment right to freedom of expression and speech is held to be greater than individual concerns about data privacy.

Article 17 of the GDPR specifies circumstances permitting data subjects to request controllers to rectify or erase data, ranging from a user's objection to the processing of data and the user's withdrawal of consent, to a situation in which the personal data is no longer necessary to the purposes for which they were collected (similar to the situation in *Google Spain*).[226] Article 17 emphasizes varying circumstances under which the user has the right to gain control over one's own data; therefore, the texts focus on the broader contexts and principles surrounding the right to be forgotten.[227] In contrast, section 1798.105 of the CCPA does not

220. A.B. 375, 2017-2018, Reg. Sess., § 1798.105(a) (Cal. 2018).

221. *Id.* § 1798.105(c).

222. *Id.* § 1798.105(b).

223. *Id.* § 1798.105(d).

224. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales, 2014 E.C.R 317, ¶¶ 93–94.

225. GDPR, *supra* note 74, art. 17.

226. *See* GDPR, *supra* note 74, art. 17(1), at (a)–(f).

227. *See id.*

discuss the particularities for which a consumer may request the Internet businesses to take down the personal information.[228] However, section 1798.105 of the CCPA does provide a greater range of exceptions under which businesses may deny individual requests to delete personal information.[229] Variances from the GDPR include circumstances allowing businesses to complete the transaction for which the personal data was collected in the context of an ongoing business relationship with the consumer.[230] The provision as stated recognizes the contractual relationship between a business and the consumer, and expressly allows businesses to use contractual duties and obligations as a defense to a consumer's request to take down an information.

Subsections 2 and 3 of Section 1798.105(d) provides for practical situations like data security breaches and impaired functionality of websites for businesses to deny the request to delete personal data.[231] The carve-outs are practical and necessary but also provide more leeway for companies to forgo complying with user requests to delete personal data in their safeguard. Also notable are provisions set out in Subsections 7 and 9, granting businesses "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" and the internal use of data "in a lawful manner that is compatible with the context in which the consumer provided the information."[232] The provisions are significant because they carve out exceptions that unequivocally acknowledge and permit business uses of personal data. Notably, internal use of personal data can refer to and encompass uses under which data is retained for businesses to generate revenue.[233] Accordingly, the exceptions demonstrate that the CCPA retains a business-friendly approach even as the law itself is an attempt at bolstering consumer protection and enforcing data privacy regulation for the benefit of California residents.

III. THE EFFECTS OF THE EUROPEAN UNION AND CALIFORNIA'S DATA PRIVACY LAWS ON BUSINESSES AND ORGANIZATIONS

A comparative study of the opt-in vs. opt-out models and the right to be forgotten provisions in the GDPR and the CCPA have illustrated the different approaches of the EU and California's data privacy laws. Although both jurisdictions have taken steps to increase individual control over personal data disseminated on the Internet, GDPR's principle-based approach to data privacy

228. A.B. 375, 2017-2018, Reg. Sess., § 1798.105(a) (Cal. 2018) ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.).

229. *See id.* § 1798.105(d), at (1)–(9).

230. A.B. 375, § 1798.105(d)(1).

231. *Id.* § 1798.105(d)(2)–(3).

232. *Id.* § 1798.105(d)(7), (9).

233. *See e.g.*, A.B. 375, § 1798.125(b) (explaining that under the financial incentive program, consumers can opt-in to give consent for businesses to legally profit from the use of consumers' personal data).

establishes a more stringent regulatory environment than the CCPA. The CCPA and its omnibus approach to privacy regulation in California is also breaking ground, with the bulk of the regulatory effects placed on businesses who must adhere to the new rules and adjust their business practices according to jurisdictional requirements. The impact on businesses are still being measured, not to mention that the CCPA went into effect quite recently on January 1, 2020. This Section attempts to review some ways businesses have already faced up to the new data privacy environment and will likely face in the years to come.

For companies doing business in the EU, they have already had to expend considerable time and effort to understand the GDPR requirements and ensure they comply with the rules after the GDPR came into effect on May 25, 2018.[234] Nevertheless, surveys show that quite a few enterprises still did not believe they have a GDPR problem or that they had the situation under control.[235] Research results show that many companies were in fact unprepared to deal with the GDPR, as there have been 59,000 data breaches reported across Europe since the introduction of the GDPR.[236] There were sixty fines recorded in 2018,[237] and ninety-one fines recorded in total in February 2019,[238] portending what is to come, that is—"a consumer movement building up steam against growing surveillance of their behavior, governments responding to consumer outrage by regulating data, and large companies like Cisco, Apple and Microsoft joining the clarion call for more such laws."[239]

Some of the lessons from the first few notable GDPR fines appear to be (1) demonstrable efforts to comply with rules count, (2) password encryption and access control matters, and (3) obtaining consent and transparency to consumers matters the most.[240] First, a German social media platform was fined only $22,812, a low figure compared to what the regulation stipulated, for a breach that compromised the personal data of 330,000 users due to its "exemplary cooperation" and demonstrable efforts to notify consumers and rectify the situation.[241] Second, encrypting passwords and ensuring access control, particularly to sensitive data, and

234. Oliver Smith, *The GDPR Racket: Who's Making Money from This $9bn Business Shakedown*, FORBES (May 2, 2018, 2:30 PM), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#6004ed8e34a2 [https://perma.cc/4HAJ-7ZTJ].

235. David Roe, *GDPR Is Tough and Set to Get Even Tougher*, CMS WIRE (Feb. 13, 2019), https://www.cmswire.com/digital-marketing/gdpr-is-tough-and-set-to-get-even-tougher/.

236. *Over 59,000 Personal Data Breaches Reported Across Europe Since Introduction of GDPR, According to DLA Piper Survey*, DLA PIPER (Feb. 6, 2019) [hereinafter GDPR Data Breach Survey], https://www.dlapiper.com/fr/france/news/2019/02/dla-piper-gdpr-data-breach-survey/ [https://perma.cc/FLZ4-SRVX].

237. Roe, *supra* note 235.

238. GDPR Data Breach Survey, *supra* note 236.

239. Roe, *supra* note 235.

240. Michael Mittel, *What We Can Learn from the GDPR's First Fines*, CMS WIRE (Feb. 14, 2019), https://www.cmswire.com/information-management/what-we-can-learn-from-the-gdprs-first-fines/ [https://perma.cc/N5SK-Z7GW].

241. *Id.*

CCTV notification to the public who may be filmed without notice, may seem basic but are often overlooked.[242] Third, the French regulators, National Data Protection Commission (CNIL), fined Google with the heaviest GDPR fine to date at fifty million dollars for failing to obtain valid user consent to obtain and process data and for providing blanket consent agreements and pre-ticked account sign-ups contrary to GDPR rules.[243] The Google fine is significant because it was investigated only after CNIL received complaints from advocacy groups like None of Your Business (NOYB) and La Quadrature du Net (LQDN)—specifically, LQDN is a group mandated by 10,000 people to refer the matter to the CNIL.[244] The advocacy groups are empowered by Article 80 in the GDPR, which reads, data subjects have the right to mandate a consumer protection body to exercise rights and lodge complaint on their behalf.[245] NOYB, a nonprofit based in Vienna, Austria and founded by privacy activist and lawyer Max Schrems, has filed complaints against streaming services including YouTube, Amazon, Netflix, and Apple.[246] Therefore, it is more than likely there will be more GDPR fines on a greater scale in the coming years.

Since the enactment of the privacy bill in June 2018, the CCPA has paved the way for other U.S. states to strengthen privacy protections across the board, but it appears that California is seeking to push the envelope even further. Recently, California State Senator Hannah-Beth Jackson and California Attorney General (AG) Xavier Becerra introduced a new bill, SB 561, which will expand the consumer's right to bring private lawsuits for violations of the CCPA.[247] As the CCPA is currently written, only the AG can sue for most violations, with an exception for private right of action under section 1798.150.[248] A consumer may only bring a private lawsuit if they first provide the business with thirty-days written notice identifying specific provisions that have been violated.[249] If passed, SB 561 is set to "(1) provide for a private right of action for all CCPA violations—not just

---

242. *Id.*

243. Connor Jones, *France Issues Google with the Heaviest GDPR Fine to Date*, IT PRO (Jan. 22, 2019), https://www.itpro.co.uk/general-data-protection-regulation-gdpr/32811/france-issues-google-with-the-heaviest-gdpr-fine-to [https://perma.cc/SUC6-UL7P].

244. Roe, *supra* note 235.

245. GDPR, *supra* note 74, art. 80.

246. *See FAQs: Who Is Behind Noyb? How Did This Project Start?*, NOYB, https://noyb.eu/faqs/ [https://perma.cc/N5V5-PD6B] (last visited Mar. 3, 2020); *see also NOYB*, WIKIPEDIA, https://en.wikipedia.org/wiki/NOYB [https://perma.cc/D8HY-457K] (last visited Mar. 3, 2020).

247. Daniel Kim & Alaap B. Shah, *Follow the Leader: California Paves the Way for Other States to Strengthen Privacy Protections*, NAT'L L. REV. (Mar. 7, 2019), https://www.natlawreview.com/article/follow-leader-california-paves-way-other-states-to-strengthen-privacy-protections [https://perma.cc/4R4S-9A5J].

248. Pursuant to § 1798.150, a private right of action is limited to consumers whose personal information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." A.B. 375, 2017-2018, Reg. Sess., § 1798.150(a)(1) (Cal. 2018).

249. *Id.* § 1798.150(b)(1).

those stemming from a data breach; (2) eliminate the 30-day period for businesses to cure after receiving notice of an alleged violation; and (3) allow the AG to publish guidance materials for businesses instead of allowing businesses' [sic] the option to seek specific opinions of the AG."[250] Therefore, SB 561, if enacted, will expose businesses to private action for damages including failure to provide consumers with proper breach notifications.

The CCPA has initiated a tidal wave for other states following suit to overhaul their privacy laws, including Hawaii, Maryland, Massachusetts, New Mexico, New York, Rhode Island, and Washington.[251] Not only that, on February 21, 2019, California also introduced AB 1130, which would expand California's definition of personal information under its breach notification law to include biometric information and government-issued identification numbers.[252] This bill updates the existing legislation passed in 2003 and would include passport numbers and driver's license information.[253] The legislation was likely prompted by the Marriott/Starwood breach last November, in which hackers stole over 500 million customer records including twenty-five million passport numbers.[254] Therefore, the aftermath of the CCPA has not abated California legislators' commitment to securing data privacy rights for individuals. It is clear that data privacy remains high on the agenda of California legislators and will likely sweep across the United States as more states jump on the bandwagon to ensure greater data protection for its residents.

CONCLUSION

As the January 1, 2020 CCPA compliance deadline has passed, the law remained unsettled and ever changing. Because the bulk of the research and writing of this Note was conducted as the compliance deadline drew to a close, the impact that CCPA implementation has on businesses and consumer rights largely remains to be seen. On April 24, 2019, the California State Assembly's Privacy and Consumer Protection Committee voted to advance five bills opposed by privacy advocates because it would undermine the CCPA and put power back into companies. The following bills would have undercut consumer privacy because (a) AB 25 allows companies to collect invasive data about their employees; (b) AB 846 increases the power of businesses to force consumers to pay for their CCPA privacy rights; (c) AB 981 allows the insurance industry to evade the consumer protections of the CCPA; (d) AB 873 weakens the definitions of "personal information" and "deidentified," which would undermine necessary privacy protections in the CCPA;

250. Kim & Shah, *supra* note 247.

251. *Id.*

252. Cal Jeffrey, *California Introduces Proposal to Expand Data Breach Notification Law*, TECHSPOT (Feb. 22, 2019), https://www.techspot.com/news/78888-california-introduces-proposal-expand-data-breach-notification-law.html [https://perma.cc/2MBK-GF9Q].

253. *Id.*

254. *Id.*

and (e) AB 1564 increases the cost of asserting privacy rights, to the detriment of consumers.[255] The disruption of economic activity by the new coronavirus shortly after the compliance deadline was passed will also leave an indelible mark on how governments, businesses, and consumers rethink and redraw the boundaries of data privacy laws in California and throughout the United States, which has ravaged the nation as this Note is being revised.

As the rapidly changing landscape of California's data privacy protection laws shows, this area of law continues to be fiercely contested in the United States, confounding attempts to predict where exactly the law will fall. By contrast, under the GDPR regime, the EU remains firm in its unwavering stance to protect EU citizens from invasions of data privacy rights. While the GDPR has become the gold standard for privacy advocates who call for strengthened data privacy protection for consumers, the CCPA is a landmark act that is yet untested, covering new grounds in the state of California, and therefore remains a fertile ground for businesses to continue the fight to weaken the CCPA. What is clear though is that the battle lines have been drawn on either sides of the Atlantic, pitting businesses against consumers who are increasingly aware and concerned about Internet privacy issues and the misuse of personal data by corporations. For now, the tide seems to have turned in favor of protecting consumer rights.

255. Hayley Tsukayama, *California Assembly's Privacy Committee Votes to Weaken Landmark Privacy Law*, ELEC. FRONTIER FOUND. (Apr. 23, 2019), https://www.eff.org/deeplinks/2019/04/california-assemblys-privacy-committee-votes-weaken-landmark-privacy-law [https://perma.cc/J9FH-S3NB].