Hastings International and Comparative Law Review

Volume 43
Number 2 *Summer 2020*

Article 6

Summer 2020

California and the European Union Take the Lead in Data Protection

Dyann Heward-Mills

Helga Turku

California and the European Union Take the Lead in Data Protection

DYANN HEWARD-MILLS[1] AND HELGA TURKU[2]

I. Introduction

California's groundbreaking privacy law, California Consumer Privacy Act (CCPA), entered into force on January 1, 2020. This law gave California residents a range of tools to protect their personal data and control over it. For example, Californians can now demand companies to disclose personal information they have collected on them, delete information upon request, and request that their data is not sold.

California, similarly to the European Union (EU), has taken the view that substantive data protection regulations are essential to safeguard the rights and freedom of individuals in a democracy.[3] The right to privacy is a fundamental human right enshrined in the Universal Declaration of Human Rights,[4] the European Convention on Human Rights,[5] and the European Charter of Fundamental Rights,[6] and the GDPR extends this right to data

1. Dyann Heward Mills is CEO of HewardMills, a minority-owned business with offices in Dublin, London, and Accra, that advises on all areas of data protection law and compliance and serves as Data Protection Officer for technology and other companies. She was previously a partner at Baker McKenzie, senior privacy counsel for GE Capital, and a senior privacy and communications lawyer at Linklaters.

2. Helga Turku has a Ph.D. in International Relations (IR) from Florida International University, a JD from UC Hastings College of the Law, and a Masters from the Middlebury Institute of International Studies. She serves as an expert consultant for HewardMills and other international organizations on legal and IR matters.

The authors would like to thank Jessica Vapnek for her thoughtful feedback and careful review of this article.

3. European Commission, "Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond—taking stock," 24.7.2019, COM (2019) 374 final.

4. UN General Assembly, *Universal Declaration of Human Rights*, Dec. 10, 1948, 217 A (III), Art. 12.

5. Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14, Nov. 4, 1950, ETS 5, Art. 8.

6. European Union, Charter of Fundamental Rights of the European Union, Oct. 26, 2012 Art. 7.

protection. In a global economy—increasingly driven by big data—personal data is not only an essential element of human dignity but also a valuable asset that needs protection.

Public awareness of data protection issues and expectations that personal data will be protected and appropriately handled has increased exponentially in recent years. Identity theft, data leaks, illegal content sharing, discriminatory practices, and intrusive surveillance are among the issues generating interest in stronger data protection laws. Legislative bodies around the world are responding to such public demand by adopting or taking steps to adopt comprehensive data protection rules.

Headlines abound regarding staggering fines imposed: $5 billion against Facebook by the US Federal Trade Commission (FTC), $170 million against Google's YouTube by the FTC and New York's Attorney General, $100 million by the US Securities and Exchange Commission against Facebook, and €57m against Google by the French Data Protection Authority. In the UK alone, the UK Information Commissioner's Office (ICO) imposed a £500,000 fine against Facebook, issued a notice of its intention to fine British Airways £183.4 million and Marriott International £99,200,396. Data protection has become a serious issue and the appropriate agencies are taking action. Companies must safeguard their consumers' data.

Although the regulatory regimes are still developing, some governments are getting out in front of the issues and taking action to protect data. This article explores the legal changes in the EU and in California, as two examples that highlight how important data protection has become both for the general public and the legislators. By comparing and contrasting these examples, the article shows how data protection laws have been fashioned in these jurisdictions and offers insights on the general trends in data protection. Any business operating in the EU and California would be wise to carefully read and abide by these new and imminent data protection laws.

II. Why Data Protection Matters

The movement toward better data protection[7] has two main drivers. First, data is a valuable asset for an entity. The rise of the big data economy

7. This article uses "data protection" and "data privacy" interchangeably. The term data protection is mostly used in EU legislative documents, while data privacy is used mostly in US legislative language. There is, however, a technical difference in the IT understanding of "protection" and "privacy," in that the former deals with protection against unauthorized use (e.g., breaches), while the latter focuses on who has authorized access (e.g., legal process). *See* Forbes Technology Council, *Data Privacy vs. Data Protection: Understand the distinction in defending your data*, Forbes, Dec. 19, 2018, https://www.forbes.com/

has in part been accelerated by the value generated by data collection, sharing, and processing. Data has been one of the main factors that has contributed in the rise of powerful tech companies like Facebook, Google, and Amazon. The normative duality of the need to use data for business growth while maintaining a healthy dose of transparency and trust with consumers has been at the center of many public discussions and has underpinned legal challenges against big data businesses.[8]

Second, privacy is one of the fundamental elements of democracy in the digital age. Unlawful data collection of a person's information "degrades the health of a deliberative democracy."[9] Questionable data collection and processing practices have the potential to "shift[] power to private organizations and public bureaucracies,"[10] thus creating a stealth power structure where the general public has little or no say. It is imperative that fair data processing practices be integrated into domestic and international laws on data protection. The need to define and create a safe space for individuals on the Internet necessitates a comprehensive normative structure that is implemented globally.

To this end, legislation in both the EU and the US has the potential to set a global trend in data protection. The key principles that characterize these pieces of legislation are: (1) limits on the collection of personal data; (2) transparency in collection and processing; (3) substantive rights for individuals subject to data collection; and (4) enforcement and accountability. The following are some key elements of the new laws in the EU and US.

The GDPR, which came into effect in May 2018, set the standard for a comprehensive data protection regime in Europe. Although the GDPR introduces a single legal framework, its provisions allow individual EU member states to enact domestic legislation defining, expanding, or restricting the scope of protection outlined in the GDPR. At the moment, all but three EU states have adopted laws to adhere to GDPR's legal framework.[11]

sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/#6f9d359d50c9.

8. Cindy Ng, *Data Privacy: Definition, Explanation and Guide*, VARONIS (Apr. 18, 2019), https://www.varonis.com/blog/data-privacy/.

9. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999).

10. *Id.* at 1612.

11. Twenty-five EU member states have adopted the required legislation, but Greece, Portugal, and Slovenia were still in the process of adopting new legislation as of the time of this publication. *See* EU Commission, *GDPR in Numbers*, https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.

While the EU has been proactive in creating a comprehensive data protection regime, laws on data protection in the U.S. are still very much developing. Absent a comprehensive federal data protection law, the CCPA is one of the first significant pieces of legislation dealing with this issue in the U.S. Just as California often leads the way in legislative matters, its CCPA, which came into effect in January 2020, may well set the standard for data protection in the country.

Although these laws have similar terminology, they differ in some key respects. Specifically, the GDPR and CCPA have different scopes, rules concerning accountability, and limitations on data collection. The GDPR requires that companies appoint a data protection officer,[12] maintain a register of processing activities,[13] and in certain circumstances where there is the possibility of a "high risk to the rights and freedoms of natural persons,"[14] the company's controller should carry out a Data Protection Impact Assessment. The CCPA, on the other hand, only has a general provision that companies should adequately handle consumers' requests to disclose or delete information.[15]

While the GDPR provides six grounds or legal bases for processing personal data,[16] the CCPA only creates a mechanism by which individuals can opt out of the sale of their personal data or request that their personal data be deleted. The CCPA also excludes from its scope the processing of certain categories of personal information, such as medical data, health data, and information processed by reporting agencies, which are covered by other US federal and state laws.

The GDPR focuses on accountability by making the controller responsible for proper implementation of the law.[17] By contrast, the CCPA focuses on transparency and includes provisions that limit selling of personal data, by obligating businesses to include a "Do not sell my personal information" link on their homepages and to provide consumers with the right to opt out in cases of mergers and acquisitions if those will materially alter how and for what purpose the data collected is used.[18]

12. 2016 O.J. (L 119) 55.

13. 2016 O.J. (L 119) 50.

14. 2016 O.J. (L 119) 53.

15. Consumer Privacy Act, Calif. Civil Code § 1798.130 (a)(6) and § 1798.135 (a)(3) (2018) [hereinafter CCPA].

16. Future of Privacy Forum, *Comparing privacy laws: GDPR v. CCPA*, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [hereinafter Future of Privacy].

17. 2016 O.J. (L 119) 35.

18. CCPA §§ 1798.135(a)(1) and (2), 1798.140(t)(2)(D).

Under both the GDPR and the CCPA, individuals have the right to access their data. However, the GDPR allows a data subject to access all processed personal data, while the CCPA grants access only for personal information collected in the 12 months preceding the request.

The expansiveness of these data protection laws reflects how legislatures are privileging the rights of their constituents against the potential economic burden to businesses (especially small ones) facing new data protection regimes. The next sections examine in more detail these laws and compare key features.

III. Data Protection under THE GDPR and CCPA – Differences and Similarities

A. Scope of Application

Data owners, data handlers, and data processors in the EU and in California have a lot at stake in the ever-changing legal landscape of data privacy. The scope of these laws varies depending on the jurisdiction, but knowledge of and compliance with these laws is particularly important in a global economy where data protection laws have extraterritorial application. The following is an overview of how the CCPA and GDPR may apply to entities operating in these jurisdictions.

The CCPA aims to increase transparency about how and why businesses collect a consumer's personal data. For the purposes of the Act, "a consumer is a natural person who is a California resident."[19] However, Assembly Bill (AB) 25 postponed by one year all CCPA requirements pertaining to employee data, except in two instances: 1) reasonable security measures to safeguard employee data; and 2) disclosure of personal information categories collected about employees and job applicants and the business purpose for which the information is collected.[20] Similarly, AB 1146 excluded from the right to opt-out vehicle or ownership information if that information is shared to effectuate a vehicle repair or recall.[21] AB 1355 excluded from coverage of the CCPA business-to-business (B2B) communications or transactions for a period of one year.[22]

The CCPA defines a business as a for-profit entity that does business in the State of California and "that collects consumers' personal information,

19. *Id.* § 1798.140(g).
20. AB-25 CCPA.
21. AB-1146 CCPA.
22. AB-1355 CCPA.

or on the behalf of which such information is collected"[23] and satisfies any of these thresholds: (1) its annual gross revenue is more than $25 million (it is not exactly clear whether this refers to the business's total revenue or just revenue in California);[24] (2) alone or in combination, it annually buys, receives, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; and (3) it derives 50% or more of its annual revenue from selling consumers' personal data.[25]

Although the CCPA limits its scope of application to companies that earn more than $25 million, paragraph 2 of the same section extends its application to entities that control or are controlled by a business with which they "share common branding."[26] Consequently, smaller companies that do not meet the $25 million annual gross revenue may be subject to CCPA provisions if they are controlled by a bigger company with which they share common branding. Conversely, the GDPR applies not only to businesses but also to public bodies and institutions. Both laws are designed to protect individuals.[27]

A critical feature of the GDPR (and one that is going to trip up a number of companies in the coming years) is that there is no requirement that the data actually be processed in the EU. Unlike the California residency requirement, the GDPR does not specifically require that the data subject be an EU resident.[28] It is sufficient that the data controller/processor[29] be either an entity established in the EU or that it monitor, or offer goods and services to, data subjects located in the EU.[30]

Unlike the general application of the GDPR, the CCPA specifically excludes from its scope "medical information," "protected health

23. CCPA. § 1798.140(c)(1).

24. Jeffrey S. King, Alidad Vakili, and Julia B. Jacobson, *Frequently asked questions about the California Privacy Act of 2018 (CCPA)*), K&L Gates (July 31, 2018), http://www.klgates.com/frequently-asked-questions-about-the-california-consumer-privacy-act-of-2018-ccpa-07-31-2018/.

25. CCPA §§ 1798.140(c)(1)(A), 1798.140(c)(1)(B), 1798.140(c)(1)(C).

26. *Id*. § 1798.140(c)(2).

27. The GDPR uses the term "data subject" while the CCPA uses the term "consumer." *See* 2016 O.J. (L 119) 33; CCPA § 1798.140 (g).

28. 2016 O.J. (L 119) 3.

29. GDPR defines controller as follows: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." Art. 4(7). Similarly, the GDPR defines "processor" as follows: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." 2016 O.J. (L 119) 8, 4.

30. 2016 O.J. (L 119) 33.

information," and "clinical trial" information.[31] The CCPA also does not apply to personal data sold to or from a consumer-reporting agency, because that is covered by the Fair Credit Reporting Act.[32] Nor does the CCPA apply to personal data processed pursuant to the Gramm-Leach-Bliley Act[33] (which requires financial institutions to explain how they share and protect consumer's personal data) or personal data processed pursuant to the Driver's Privacy Protection Act (which governs how privacy and disclosure of personal data is gathered by state Departments of Motor Vehicles).[34] Moreover, the CCPA excludes from its applicability "publicly available" information, which is defined as "available from federal, state, or local government records."[35] The GDPR, on the other hand, applies to publicly available data. Hence, if a data controller collects personal data from public sources, the GDPR will apply.[36] On the other hand, both the GDPR and the CCPA do not apply to anonymous[37] or deidentified/aggregate[38] consumer information.

The CCPA grants a right to privacy and allows a consumer the right to request a business to disclose specific information that it collects,[39] the business purpose for which it collects or sells[40] information, and the categories of third parties with which this personal data is shared.[41] However, in its definition of what constitutes selling personal data, the CCPA excludes four scenarios. The first is where a consumer uses or directs a business to intentionally disclose personal information or uses the business to intentionally interact with a third party.[42] Intentional interaction does not include "[h]overing over, muting, pausing or closing a given piece of content."[43] In other words, the consumer's intent to interact with a third party

31. CCPA § 1798.145(c).

32. *Id.* § 1798.145(d).

33. *Id.* § 1798.145(e).

34. *Id.* § 1798.145(f).

35. *Id.* § 1798.140(o)(2).

36. 2016 O.J. (L 119) 41.

37. 2016 O.J. (L 119) 5.

38. CCPA § 1798.140(s)(2).

39. CCPA § 1798.140(e) defines collecting as: "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."

40. CCPA § 1798.140(t) defines selling as: "renting, releasing, disclosing, disseminating, making available transferring, or otherwise communicating . . . a consumer's personal information . . . for monetary or other valuable consideration."

41. *Id.* § 1798.110(a).

42. *Id.* § 1798.140(t)(2)(A).

43. *Id.*

must be deliberate, and the third party may not sell the consumer's personal data unless it is consistent with the CCPA.[44]

The second scenario that the CCPA excludes from its scope is where the business shares the consumer's personal data with a third party for the purpose of alerting them that the individual has opted out of the sale of personal data.[45] The third scenario is where the business shares a consumer's personal data "that is necessary to perform a business purpose,"[46] and the fourth is where the business transfers a customer's personal data to a third party as part of a merger, acquisition, or other related transaction.[47] In this last scenario, the data is an asset that cannot be used for other purposes other than those already agreed upon at the time of the collection, unless the business has the consumer's consent.[48]

The GDPR, on the other hand, has a much broader scope and defines processing activities as "any operation . . . which is performed on personal data . . . whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[49] However, the GDPR excludes two kinds of processing activities from its applicability: (1) data processing conducted through a non-automated means that is not part of a filing system;[50] and (2) processing conducted "by a natural person for a purely personal or household purpose."[51] The purpose of this detailed definition is to protect individuals no matter the technology used. In other words, whether an entity files personal data in an automated or non-automated manner, that data falls under the protection of the GDPR.

Both the GDPR and the CCPA do not apply to law enforcement and national security entities, but businesses providing services to such entities may fall under the provisions of these laws.[52] It is important that businesses working with law enforcement or national security agencies check what they can and cannot do legally.

44. *Id.*
45. *Id.* § 1798.140(t)(2)(B).
46. *Id.* § 1798.140(t)(2)(C).
47. *Id.* § 1798.140(t)(2)(D).
48. *Id.*
49. 2016 O.J. (L 119) 33.
50. 2016 O.J. (L 119) 3.
51. 2016 O.J. (L 119) 32.
52. Future of Privacy & OneTrust DataGuidance, *supra* note 16, at 10.

B. Legal Basis for Processing Personal Data under the GDPR

Under EU data protection law, there must be a lawful basis for the processing of personal data, unless an exception applies. The GDPR lists six contexts where data processing can be lawful: (1) consent;[53] (2) processing is necessary to perform a contract to which the data subject is a party, or other tasks related to that contract;[54] (3) the data controller's compliance with legal obligations;[55] (4) necessity relating to the vital interests of the data subject or of another natural person;[56] (5) public interest or in the "exercise of official authority vested in the controller";[57] and (6) processing is necessary for the legitimate pursuits of the controller or a third party, except where these interests are overridden by the fundamental rights and freedoms of data subjects, especially when they are children.[58]

By contrast, the CCPA does not enumerate precise legal grounds when data processing is allowed, but it states that businesses must inform customers before collecting, selling, or disclosing information and must provide an opt-out mechanism when data is being sold or disclosed to third parties. In this respect, the GDPR is much more stringent with respect to how and why data is collected. Under its regime, personal data may only be processed if and to the extent that an enumerated legal basis applies.[59]

Unlike the CCPA where consumers may only ask the business not to sell their data, the GDPR gives data subjects the right to withdraw consent[60] and object[61] at any time to processing of their personal data. Even if the personal data is lawfully processed for a public interest reason or to advance other legitimate interests of a controller or third party, the data subject can object to such processing. It is for the controller to demonstrate that its

53. 2016 O.J. (L 119) 36.

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.* Under the GDPR, children have specific protection "as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data." 2016 O.J. (L 119) 7.

59. Detlev Gabel & Tim Hickman, *Chapter 7: Lawful basis for processing – Unlocking the EU General Data Protection Regulation*, White & Case (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection.

60. 2016 O.J. (L 119) 12.

61. 2016 O.J. (L 119) 45; 2016 O.J. (L 119) 13.

compelling legitimate interest overrides the fundamental rights and freedoms of the data subject.[62]

C. Processing Special Categories of Personal Data and Biometric Data

Article 9 of the GDPR prohibits processing of special categories of personal data, such as information that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[63] The CCPA includes biometric information in its protected personal information list, however it does not give it the same heightened protection as GDPR.[64] Furthermore, under the CCPA biometric data is not considered public information and may only be collected with the permission of the consumer.[65]

Although the GDPR provides heightened protection for special categories of personal data that may reveal sensitive information about a person, there are some instances where collecting and processing this data is allowed. These exceptions are:

(1) the data subject has given explicit consent and that consent is not otherwise prohibited by another EU or member state law;[66]

(2) processing is necessary to carry out obligations or to exercise specific rights of the controller or rights of the individual in regards to employment, social security, and/or social protection;[67]

(3) processing is necessary to protect the vital interests of the individual or another natural person where the data subject is physically/ legally incapable of consenting;[68]

(4) the data is handled in the course of legitimate activities by a foundation, association, or other not-for-profit entity with a political, philosophical, religious, or trade union goal;[69]

62. 2016 O.J. (L 119) 46.
63. 2016 O.J. (L 119) 38.
64. Future of Privacy & OneTrust DataGuidance, *supra* note 19, at 13.
65. CCPA § 1798.140 (o)(2).
66. 2016 O.J. (L 119) 38.
67. *Id.*
68. *Id.*
69. *Id.*

(5) the data processing relates to information that is made manifestly public by the data subject;[70]

(6) processing is necessary in a legal action or whenever courts are acting in their judicial capacity;[71]

(7) data processing is necessary for issues related to substantial public interest;[72]

(8) processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, provision of health care, assessment of working capacity of an employee, or the management of health/social care systems in the EU or a member state;[73]

(9) processing is necessary in the context of public health;[74]

(10) processing is necessary for archiving purposes related to issues of public interest, scientific, historical, or statistical research.[75]

In other words, sensitive personal data cannot be collected or processed unless one of these exceptions applies.

D. Child Consent

The GDPR and CCPA emphasize special protection for children and provide specific provision for data protection where children are concerned. The GDPR recognizes children as "vulnerable natural persons"[76] that merit special protection. Parents or guardians are to provide consent for individuals under the age of 16.[77] While the EU member states can lower that age, they cannot go below age 13.[78] Data controllers are required to make reasonable efforts to verify that consent to collect and process data is indeed given by a parent/guardian.[79] When online preventive or counseling services are offered to a child, parental/guardian consent is not necessary,[80] thus allowing a minor to be informed without the knowledge and/or permission of a parent or guardian.

70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. 2016 O.J. (L 119) 15. 2016 O.J. (L 119) 7.
77. 2016 O.J. (L 119) 37.
78. *Id.*
79. *Id.*
80. 2016 O.J. (L 119) 7.

The CCPA grants consumers under the age of 16 the right to opt in to have their information sold if a business has "actual knowledge" that the consumer is under the age of 16. Under the CCPA, "actual knowledge" of the consumer's age means that the business willfully disregards the consumer's age. A business in California may not sell personal information of consumers when they are under the age of 13, unless the business has affirmative authorization by the consumer's parent or guardian.[81]

The biggest difference between the GDPR and the CCPA is that in the EU, the law does not provide for any exceptions for a controller that is not aware that it is actively collecting the personal data of a child or providing services to a child.[82] Hence, the penalties for collecting and/or processing personal data of children can be far more serious in the EU.

Another tangential issue is that under the GDPR, any information or communication directed at a child should be written in plain language and clear to understand.[83]

E. Individual Rights

The GDPR grants data subjects various rights with regard to personal data processing and imposes obligations on data controllers to respect the rights granted in the GDPR. Similarly, California also enumerates its residents' rights to privacy.

Right to know – The GDPR CCPA obligate entities handling personal data to inform individuals when collecting and processing their information. The GDPR distinguishes between notices given to individuals when their information is collected directly from them[84] and when it is obtained using other sources.[85]

Under the GDPR, individuals are to be informed about the categories of data processed, the purpose of such processing, the existence of their rights, and where applicable, how to contact the DPO.[86]

The CCPA, on the other hand, gives consumers the right to request that a qualifying business disclose "the categories and specific pieces of information" it collects about that person, the source from which the personal

81. CCPA § 1798.120(d).

82. 2016 O.J. (L 119) 36; 2016 O.J. (L 119) 37; 2016 O.J. (L 119) 39; 2016 O.J. (L 119) 56; 2016 O.J. (L 119) 68; 2016 O.J. (L 119) 7; 2016 O.J. (L 119) 11; 2016 O.J. (L 119) 15.

83. 2016 O.J. (L 119) 11.

84. 2016 O.J. (L 119) 40.

85. 2016 O.J. (L 119) 41.

86. 2016 O.J. (L 119) 40; 2016 O.J. (L 119) 41.

information was collected, its business purpose,[87] and—if a business sells/discloses that information to third parties the categories of third parties with whom the business shares this information.[88] In case of a third-party sale, the consumer has the right to opt out. Businesses must include a link to the "Do not sell my personal information" page where consumers may exercise this right.[89]

Under the CCPA, a business should also make "reasonably accessible"[90] disclosures on its online privacy policy, including a description of consumers' rights, methods for a consumer to submit a verifiable request,[91] and lists of categories of personal information collected about consumers[92] that it has sold[93] and that it has disclosed (or not disclosed) about consumers for a business purpose—all of these in the previous 12 months.[94]

While GDPR states that this information should be provided to individuals at the time when personal data is obtained,[95] the CCPA states that the consumer shall have the right to be informed "at or before the point of collection."[96]

Moreover, under the right to know, the GDPR gives data subjects the right to be informed about their other rights.[97] The CCPA has a similar provision, which requires that businesses describe a consumer's rights.[98]

Right of access – The CCPA and GDPR create a right to access, which enables individuals to have full understanding of the data an entity holds about them. Under the GDPR, individuals may access all their personal data.[99] In California, once the CCPA comes into effect, a consumer can only access information collected 12 months prior to the request.[100] Upon

87. CCPA § 1798.100.

88. *Id.* § 1798.110(c)(5).

89. *Id.* § 1798.135(a).

90. *Id.* § 1798.130(a)(5).

91. *Id.* § 1798.130(a)(5)(A). Under § 1798.140(y), a verifiable consumer request is made "by a consumer or on behalf of the consumer [whom] the business can reasonably verify . . . to be the consumer about whom the business has collected personal information."

92. *Id.* § 1798.130(a)(5)(B).

93. *Id.* § 1798.130(a)(5)(C)(i).

94. *Id.* § 1798.130(a)(5)(C)(ii).

95. 2016 O.J. (L 119) 40.

96. CCPA § 1798.100(b).

97. 2016 O.J. (L 119) 43.

98. CCPA § 1798.130(a)(5).

99. 2016 O.J. (L 119) 43.

100. CCPA § 1798.130(a)(3).

receiving a verifiable consumer request, the business must provide free of charge "specific pieces of personal information."[101]

Right to be forgotten – The CCPA and GDPR provide for the right of individuals to request that their personal data be deleted. Though the right can be exercised free of charge, a reasonable fee may be charged in some situations.[102] The GDPR limits this right to cases where the processing is no longer necessary or consent has been withdrawn, or where the personal data is no longer necessary for the purposes for which it was collected.[103] The controller is not obligated to comply with a request to delete personal information when the data is necessary for the exercise of free speech, compliance with EU or member state law, or public interest in the area of public health, scientific research, or exercise/defense of legal claims.[104] Nevertheless, the GDPR creates a broad right to erasure, and entities subject to this law should be prepared for the possibility of receiving a multitude of requests for personal data erasure.

The CCPA does not limit the right to be forgotten to specific cases, and there is no specific requirement that the consumers justify their request.[105] Like the EU law, under the CCPA the right to request that personal information be deleted is limited in certain situations involving free speech, security, research, and other legal obligations.[106] Critics point out that the exceptions are too broad, thus potentially diminishing this right for Californians.[107] Moreover, while under the EU law the data subject is entitled to the deletion of all their data, the CCPA only applies to data collected from the consumer, thus leaving out data that has been collected through third parties.[108]

The deadline for complying with a request for personal data erasure under the CCPA is 45 days, which may be extended for an additional 45 days.[109] Under the GDPR, the deadline is one month, which can be extended to two months.[110]

101. *Id.*§ 1798.100(a).

102. 2016 O.J. (L 119) 40; CCPA § 1798.145(g)(3).

103. 2016 O.J. (L 119) 43.

104. 2016 O.J. (L 119) 44.

105. CCPA § 1798.105(c).

106. *Id.* § 1798.105(d).

107. Steven R. Chabinsky & F. Paul Pittman, *CCPA and GDPR: Comparison of certain provisions*, White & Case Technology Newsflash (Sept. 7, 2018), https://www.whitecase.com/publications/article/ccpa-and-gdpr-comparison-certain-provisions.

108. *Id*.

109. CCPA § 1798.130(a)(2).

110. 2016 O.J. (L 119) 11.

Right to rectification – The GDPR provides that data subjects have the right to obtain the rectification of inaccurate personal data.[111] Individuals may supplement their incomplete data through a statement. The CCPA does not have specific language on this issue.

Right to opt out – The GDPR and the CCPA ensure that the consumer is able to object to the processing of their data. As noted, the CCPA requires that a business provide a "Do not sell my personal information" link on their website.[112] Moreover, a third party can only sell an individual's information if it provides California residents with explicit notice and the opportunity to opt out.[113] As explained earlier, under the CCPA consumers can only opt out of the sale of their data if the transaction does not fall under the definition of "selling."[114] By contrast, the GDPR allows individuals to object to data processing by withdrawing consent or by exercising their right to object.[115] While the GDPR uses a different legal scheme, this does not mean that the EU right to opt out is any less stringent.

Right to data portability – The GDPR provides that upon request personal data should be transmitted to another controller/business without hindrance.[116] On the other hand, the CCPA obligates businesses to provide personal data upon a verifiable request by a consumer in a portable and readily usable format, which then can be used by the consumer to transmit that information to another entity.[117] As such, the CCPA does not go as far as the GDPR in making a business transfer data to another business.

While the GDPR treats this right as a separate right,[118] under the CCPA data portability is included in the right to data access. The consumer can only make a verifiable request to receive this information twice in a 12-month period.[119]

Right not to be discriminated against – In California, consumers may not be discriminated against because they exercise their rights under the CCPA.[120] The GDPR does not include a specific provision to this effect, but the concept is implicit in its general principles, such as the prohibition

111. 2016 O.J. (L 119) 45.
112. CCPA § 1798.135(a).
113. *Id.*
114. CCPA. § 1798.140(t)(2).
115. GDPR Art. 12, Art. 21, Recital 70.
116. 2016 O.J. (L 119) 45.
117. CCPA § 1798.100(d).
118. 2016 O.J. (L 119) 45.
119. CCPA § 1798.100(d).
120. *Id.* § 1798.125(a)(1).

against processing that may adversely affect the rights and freedoms of the data subject.

F. Restrictions

The rights articulated in the GDPR and the CCPA are not absolute. Article 23 of the GDPR states that EU member states may restrict the scope of the data subjects' rights and the data controllers' obligations. Specifically, these rights and obligations are restricted when necessary and proportionate to safeguard a democratic society's: (1) national security;[121] (2) defense;[122] (3) public security;[123] (4) prevention, investigation, or prosecution of criminal activities;[124] (5) preservation of other important objectives, i.e., economic and financial interests;[125] (6) protection of judicial independence and judicial proceedings;[126] (7) prevention, investigation, and prosecution of ethical breaches for regulated professions;[127] (8) monitoring, inspection, or regulatory functions connected to the exercise of official authority in matters related to national security, monetary interests, and regulated professions (e.g., doctors, lawyers),[128] (9) the protection of data subject or the rights and freedoms of others;[129] and (10) the enforcement of civil law claims.[130]

Any EU or national law that restricts the data subject's enumerated rights to adhere to GDPR Article 23, should consider the purpose of the data processing, the affected categories of data, the scope of the restriction, any safeguards to prevent abuse, the specification of the controller or categories of controllers, the applicable retention period, and the risks to the rights and freedoms of the data subject, and the controller must inform the data subject about the restrictions unless that is prejudicial to the purpose of the restriction.[131]

Recital 73 of the GDPR states that Union or member state law may impose additional restrictions. However, any such restrictions should be

121. 2016 O.J. (L 119) 46.
122. 2016 O.J. (L 119) 46.
123. 2016 O.J. (L 119) 46.
124. 2016 O.J. (L 119) 47.
125. *Id*.
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.*

limited to what is necessary and proportionate in a democratic society, thus safeguarding basic human rights and fundamental freedoms.[132]

Similarly, under the CCPA, businesses are not required to delete the consumer's information where the information is necessary to carry out the transaction for which the data was collected, detect security incidents, exercise free speech, comply with state law, exercise/defend legal claims, or engage in scientific or historical research.[133] The obligations under the CCPA do not restrict a business's ability to comply with local/state/federal law, comply with legal requests, exercise or defend legal claims, process deidentified/aggregate consumer information, or collect or sell a consumer's personal information if the commercial activity takes place wholly outside of California.[134] While some of these restrictions are broad, a business should still ensure that consumers are informed about their rights and the business's privacy policies.[135]

G. Accountability under GDPR – Data Protection Officers

EU and California law differ substantially with regard to accountability. Under the GDPR, public authorities (except courts acting in their judicial capacity) or entities that regularly and systemically monitor data subjects on a large scale must appoint a Data Protection Officer (DPO); maintain a register of processing activities; and, in certain cases, create a data protection impact assessment.[136] By contrast, the CCPA merely states that companies should be prepared to deal with consumer requests and does not provide more specific accountability-related obligations.[137]

The GDPR requires that DPOs work independently and be bound by confidentiality when performing their duties, in accordance with EU or member state law.[138] The DPO may not have a conflict of interest while serving the data controller/processor, thus ensuring that GDPR and state law obligations are impartially implemented while serving the best interests of both the data subjects and the entities that hire them.

132. *Id*. 2016 O.J. (L 119) 14.
133. CCPA § 1798.105(d).
134. *Id.* § 1798.145(a).
135. *Id.* § 1798.130(a)(5)
136. 2016 O.J. (L 119) 116.
137. CCPA § 1798.130.
138. 2016 O.J. (L 119) 56.

H. Enforcement and Penalties

The GDPR and the CCPA provide for monetary penalties in cases of noncompliance. Depending on the violation, a data protection authority in an EU member state can issue a fine up to 4% of the global annual turnover or €20 million, whichever is higher. Article 83(2) of the GDPR states that the penalty depends on the "the nature, gravity and duration of the infringement." In California, the penalty can be up to $7,500 for each intentional violation.[139]

Both the CCPA and GDPR provide for civil remedies for individuals. Under the GDPR, individuals can seek both monetary and non-monetary remedies for any type of violation.[140] The CCPA, on the other hand, only allows individuals to pursue civil remedies when nonencrypted or nonredacted personal information is subject to unauthorized access, theft, or disclosure as a result of a business's failure to implement appropriate security measures.[141] A consumer may recover up to $750 per incident or actual damages, whichever is greater, seek injunctive or declaratory relief, or pursue any other relief that the court deems proper.[142]

However, prior to initiating any action against a business whether on an individual or a class-wide basis, consumers need to provide the business with 30 days' notice that identifies the alleged violation. If the business is able to cure the alleged violation within 30 days, no further legal action can take place. The consumer must also notify California's Attorney General within 30 days after an action is filed.[143] The Attorney General then can decide whether to prosecute the action.[144] If the individual has suffered pecuniary damages, no notice is required prior to initiating a legal action to recover those damages.[145] In other words, the CCPA limits private claims to breaches of unencrypted/ unredacted data caused by a business's negligence. Otherwise, the Attorney General acts as the enforcer of the Act. Although the CCPA comes into effect in January 2020, the Attorney General may not

139. CCPA § 1798.155(b).
140. 2016 O.J. (L 119) 80.
141. CCPA § 1798.150(a)(1).
142. *Id.*
143. *Id.* § 1798.150(b)(2).
144. *Id*.
145. *Id.* § 1798.150(b)(1).

begin enforcing the Act until July 1, 2020 (or six months after implementation, if that is after January 2020).[146]

IV. Conclusion

The right to privacy has long been recognized as a fundamental human right. Recent data protection regimes around the world are a natural step toward better protection of that fundamental right and the protection of personal freedoms in a democratic society.

The data protection laws in Europe and California show that the legislators are actively seeking to create and strengthen individual rights. In the age of technology where personal data has real value for marketing, product development, and related fields, it is only logical that such assets be legally protected.

In the last few years, data protection has reached a number of thresholds, both legislatively and in the arena of public opinion. Questions about inappropriate use of data, breaches, and unauthorized collection of personal information have become important issues in policy and legal circles. The trend toward strategic and normative changes in the law and public opinion is surely on the rise, and will most likely continue, as individuals no longer have to sacrifice their personal information in order to function in the age of technology. The GDPR and other national data protection laws in Europe have set standards that are sure to be followed by other jurisdictions in an interconnected world. Closer to home, the CCPA is on the horizon and will have cataclysmic effects in California and beyond.

146. Christina Kroll, *CCPA: Consumers and Right to Sue*, Mind Your Business (May 31, 2019), https://www.mindingyourbusinesslitigation.com/2019/05/ccpa-consumers-and-the-right-to-sue/.

***