Data Protection Laws Are Here, But What Do They Mean for California Businesses?

Jordan Yallen and Kevin D. DeBré

Jordan Yallen is a second-year Juris Doctor candidate at Loyola Law School Los Angeles. Jordan is a Staff Editor of the Loyola of Los Angeles Law Review and the Social Events Chair of Loyola's Innovation, Entrepreneurship, and Start-Ups Club. In the summer of 2018, Jordan interned for Ashley Boardman at Silicon Beach Legal, PLC, where he focused on researching the GDPR and analyzing organizational policies and protocols regarding compliance with the regulation.

Kevin D. DeBré is a partner with Stubbs Alderton & Markiles, LLP in Los Angeles, California, where he is the chair of the firm's Intellectual Property and Technology Transactions Practice Group.

If information is the lifeblood of every business, then data is the oxygen enabling businesses to thrive. Digital technologies have simplified the collection, analysis, storage, sharing, and manipulation of data. Along with these improvements, digital technologies have also brought a surge of new regulations governing how companies may use collected data. Recent laws enacted to protect consumer privacy and address data security risks are just the first wave of a vast regulatory regime within which most businesses must soon operate. These companies will rely upon their counsel to ensure that they are in compliance with this fluid landscape of privacy laws. This article highlights the responsibilities associated with collecting and using personal data through an analysis of two significant, recently adopted privacy laws: the European Union's General Data Protection Regulation ("GDPR") and the California Legislature's recent passage of Assembly Bill No. 375, the California Consumer Privacy Act of 2018 ("CCPA").

I. GDPR: This Year's Import from the European Union

The GDPR, effective on May 25, 2018, reflects some of the most significant reforms of consumer data protection laws to date. The GDPR's coverage of "data subjects" includes "any information relating to an identified or identifiable natural person" residing in the European Union ("EU").[1] However, the GDPR's reach extends beyond the EU if a business (1) processes the personal data of EU residents in connection with offering goods or services or (2) monitors behaviors of data subjects within the EU.[2] A company need not be located in the EU to be subject to the GDPR.

A. GDPR Compliance

California-based businesses that process personal data or monitor behaviors of EU residents must comply with the GDPR's stringent consent requirements and expanded individual rights in controlling the use of personal data, implement new data storage systems and policies, and potentially appoint a specific GDPR representative.

Processing consists of storing, organizing, retrieving, transmitting, or any other action, automated or not, performed on personal data.[3] Businesses outside of the EU are subject to GDPR compliance as either a "data processor," if they actually process this data, or as a "data controller," if they direct "the purposes and means of the processing."[4] Monitoring behaviors of EU residents "includes the tracking of individuals online to create profiles, including where this is used to take decisions to analyse/predict personal preferences, behaviours and attitudes."[5]

Before collecting any data, controllers must inform data subjects of the legal basis and purposes for

processing personal data, contact information for the controller or a representative, "the legitimate interests pursued by the controller … or third party," the types of personal data being collected, and to whom the controller will provide this data.[6] This information must be presented "in a concise, transparent, intelligible and easily accessible form," often as a privacy policy, "using clear and plain language."[7]

Consent to collecting data from a data subject should be evidenced by "a clear affirmative act."[8] Usually, this consent is sought when a data subject is required to complete a registration form to access a website's services. Consent is provided when the data subject checks a box accompanied by a statement disclosing the purposes for which the data subject's information will be processed and the data subject submits the completed registration form. A data subject must provide additional consent when (1) there is more than one agreement—such as a terms of use and a privacy policy—and (2) "the processing has multiple purposes."[9] In addition, parental consent is required for children under the age of sixteen; however, EU Member States may lower the age threshold to as low as thirteen years old.[10] It is the controller's responsibility to "make reasonable efforts to verify … that consent is given or authorised by" a child's parent or guardian, "taking into consideration available technology."[11]

After consent is given, the consenting data subjects have rights to control the use of their personal data when a data controller processes or collects their personal data. Data subjects have the right to revoke "consent at any time," which would require the data controller to stop using their data.[12] In addition, data subjects have the "right to be forgotten": upon a data subject's request, the data controller must delete the personal data collected from the data subject.[13] Further, data subjects may require data controllers to correct information in collected data, and may restrict what data controllers can do with their collected data.[14] To fulfill a data subject's request to correct their information, controllers must store data in a manner that enables personal data to be easily transmitted to the data subject and in a form that is viewable.[15] A data controller must comply with a request within one month of receipt.[16] Businesses that are not prepared to fulfill such requests should start putting these procedures in place.

Depending on the amount of EU resident data that is processed or monitored, a business may be required to designate a data protection officer or EU-based representative. Data protection officers are generally needed only for California businesses that monitor data subjects on a "regular and systematic" basis, which includes all forms of online tracking and profiling (such as those conducted for behavioral advertising and email retargeting),[17] or whose "core activities … consist of processing on a large scale of special categories," such as race, religion, sexual orientation, and genetic information.[18] If a company is required to designate a data protection officer, there is no need to establish a dedicated position within the organization. As long as the data protection officer can fulfill the obligations to inform, advise, and monitor a company's compliance with the GDPR, the position may be contracted to an outside party serving on behalf of multiple businesses, or this responsibility may be assigned to an existing staff member.[19]

Further, businesses that fall within the GDPR's scope, but are located outside of the EU, must appoint a representative in the EU, unless the "processing . . . is occasional" and does not consist of any sensitive "special categories of data."[20] The regulation does not provide a threshold for what constitutes "occasional" processing, and it is too soon to know how regulators will interpret this requirement.

Finally, the controller is responsible for creating guidelines "to ensure that the personal data [is] not kept longer than necessary."[21] As long as data subjects are identifiable by the collected data, the data may only be used and stored in accordance with the duration required for the purposes for which it was collected.[22] The processing of anonymous information is not within the scope of the GDPR, but personal data that has undergone pseudonymization—a process after which additional information is necessary to identify the data subject—is still considered personally identifiable data.[23] Businesses must delete personal data when it is no longer necessary for processing or legal purposes or when a data subject objects to or withdraws consent for processing.[24]

B. GDPR Interpretation and Enforcement

With time, enforcement actions will provide guidance as to how regulators will interpret the GDPR's

requirements, and application of these requirements should become more certain and predictable. For now, however, attorneys can offer their clients little insight concerning the risks of violating the GDPR. The regulation states that any business that fails to comply may be subject to fines, judicial remedies, and liability for damages.[25] "Each [EU] Member State" is responsible for establishing "one or more independent public [supervisory authorities] to be responsible for monitoring," enforcing, and imposing fines for violations of the GDPR.[26] These supervisory authorities may levy fines of up to €20 million or 4% of "worldwide annual turnover of the preceding financial year, whichever is higher."[27] On September 28, 2018, Facebook announced a data breach affecting approximately thirty million accounts. This breach, along with three recent cases discussed below, may soon offer clues as to how regulatory authorities will apply the GDPR's penalties.[28]

Recent reports of the first GDPR enforcement notice indicate that AggregateIQ may face the maximum allowable fines under the regulation.[29] The Information Commissioner's Office ("ICO"), the UK body enforcing GDPR compliance, issued the notice to AggregateIQ, a Canadian firm specializing in targeting voters through advertisements.[30] The notice claimed that the firm improperly processed and retained personal data that was provided to AggregateIQ by notorious pro-Brexit groups and collected prior to the GDPR's effective date.[31] After the GDPR went into effect, the ICO claimed that AggregateIQ continued to process "personal data in a manner inconsistent with data subjects' knowledge, for purposes which they would not have expected" when collected originally, "and without a lawful basis for that processing."[32] While AggregateIQ is appealing these claims, the notice demands that the firm "[c]ease processing any personal data of UK or EU citizens obtained from UK political organisations . . . for the purposes of data analytics, political campaigning or any other advertising purposes."[33] The outcome of this case will be significant in determining how failure to comply with the GDPR will affect non-EU-based businesses.

Another major test of GDPR enforcement will likely be in response to the British Airways data breach announced in early September of this year.[34] While it remains early in the investigation, it appears that data from 380,000 credit cards were stolen. If true, this breach could result in fines of as much as £825 million.[35] In addition to fines imposed by the ICO, British Airways could be liable for an enormous damages award in a class action lawsuit if the airline is "found to have failed to protect their [customers'] personal data properly."[36]

In the United States, GDPR-related litigation was brought by a Nielsen Holdings shareholder over claims that the ratings service misled shareholders about the impact of GDPR compliance on its business.[37] The lawsuit alleges that Nielsen initially reported that fallout from compliance with the GDPR would be minimal from a financial perspective.[38] However, after missing fiscal projections for the second quarter of 2018, Nielsen blamed the GDPR for the company's woes and subsequently sustained a twenty-five percent loss in market capitalization in July.[39] While the Nielsen lawsuit did not arise out of a GDPR violation, it demonstrates the GDPR's broad impact on companies located anywhere in the world.

II. CCPA: California Takes the Lead in the United States and Follows the EU

A. U.S. Privacy Laws Before the CCPA

In addition to the GDPR, prior privacy legislation and recent revelations about abusive data collection practices have laid the foundation for the passage of the California Consumer Privacy Act of 2018. The CCPA is California's recent effort to protect consumer privacy by regulating how companies use the data they collect. Prior to the CCPA, legislatures in Illinois, Massachusetts, and New York took steps to protect online privacy and address cybersecurity risks.[40]

Illinois enacted the Biometric Information Privacy Act in 2008 in response to the growing usage of biometric identifiers.[41] The act protects personal biometric data, including "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," by establishing guidelines for acquiring, storing, and deleting biometric data.[42]

In 2010, Massachusetts implemented the Standards for the Protection of Personal Information of Residents of the Commonwealth.[43] This law applies to anyone who "own[s] or license[s] personal information about a resident of the Commonwealth," such as a Massachusetts resident's name, in connection with a Social Security number, driver's license or other identification card,

or credit cards and other financial information.[44] The Massachusetts law mandates that those within its scope must "maintain a comprehensive information security program" by authenticating users, restricting access, encrypting transmissions, and monitoring protocols.[45]

Furthermore, New York enacted the Cybersecurity Requirements for Financial Services Companies in 2017 to combat "the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors."[46] New York's cybersecurity law requires those operating under banking, insurance, or financial services laws to implement cybersecurity policies and protocols; appoint a chief information security officer; and assess, monitor, and audit cybersecurity systems.[47]

California's turn to regulate privacy law began with a ballot initiative known as The Consumer Right To Privacy Act of 2018.[48] This initial incarnation of the CCPA was strongly opposed by technology companies, including Facebook, for being a "flawed" measure.[49] However, Facebook ended its efforts to oppose the act after Mark Zuckerberg appeared before Congress in April of 2018 to account for the Cambridge Analytica data breach.[50] In a last minute effort, California's legislature narrowly passed the CCPA so that the organization behind the initiative, Californians for Consumer Privacy, would drop the measure from the November 2018 ballot.[51]

B. The CCPA: A Work in Progress

California's road toward protecting privacy rights began in the 1972, with the amendment of California's Constitution to include "the right of privacy among 'inalienable' rights of all people."[52] Since then, California's Legislature has implemented multiple measures to protect privacy "including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, a California Law intended to give Californians the 'who, what, where, and when' of how businesses handle consumers' personal information."[53] A need for increased privacy regulation became apparent after Cambridge Analytica's improper use of the personal data of Facebook's members "highlighted that our personal information may be vulnerable to misuse when shared on the Internet."[54]

California Governor Jerry Brown signed the CCPA into law on June 28, 2018, giving businesses until January 1, 2020, to comply with "the most comprehensive privacy legislation ever passed in the United States."[55] The legislative intent behind the CCPA is to provide consumers with "an effective way to control their personal information."[56] The act aims to achieve this by granting Californians the rights to (1) know what personal information businesses collect, (2) request that their data be deleted, (3) know what information is sold or disclosed to third parties and the identity of those third-parties, (4) "opt out" of the sale of their information, and (5) exercise their rights under the CCPA and receive the same prices and services as those who do not.[57]

To comply with the CCPA, businesses must disclose (1) what information is being collected before or at the time of collection, (2) that the consumer has the right to request deletion of their information, and (3) who will be given access to the consumer's information.[58] When a California consumer asks what specific information has been collected, the company collecting this information must provide the consumer with their collected data, without charge, up to twice every twelve months.[59] To do this, data must be stored in a manner that is easily portable and accessible to consumers.[60] Further, businesses that sell the personal information of consumers must "[p]rovide a clear and conspicuous link on the business's Internet homepage, titled 'Do Not Sell My Personal Information,'" to allow consumers to opt out of the sale of their information.[61]

The CCPA's scope extends to any business that processes or collects personally identifiable information of California residents and (1) has "annual gross revenues in excess of twenty-five million dollars," (2) purchases or sells "personal information of 50,000 or more consumers, households, or devices," or (3) "[d] erives 50 percent or more of its annual revenues from selling consumers' personal information."[62]

Consumers may bring lawsuits against businesses that violate the CCPA only in connection with data breaches; only the California Attorney General can enforce CCPA violations.[63] Businesses within the scope of the CCPA are liable for civil damages when a failure "to implement and maintain reasonable security procedures" results in a breach involving the personal

information of California residents.[64] One way a company may be able to minimize this potential liability would be to demonstrate that it made a reasonable effort to implement the CCPA's standards. A business can seek the opinion of the Attorney General for guidance on how to comply with the provisions of the CCPA.[65] Taking reasonable steps to comply, following up with the Attorney General, and following any advice the Attorney General provides may serve as a mitigating factor in adjudicating a company's liability.

C. CCPA's First Amendment

On September 23, 2018, less than three months after signing the CCPA, Governor Brown approved the first Amendment to the Act, Senate Bill No. 1121 (the "Amendment").[66] The Amendment aims to clarify the Act and extends enforcement of the CCPA for up to six months following its effective date.[67] Further, it carves out exemptions for institutions complying with other federal and state acts, including financial, healthcare, and insurance-related regulations such as the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, HIPPA, and the Driver's Privacy Protection Act.[68]

The Amendment's corrections and clarifications include the definition of personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably linked, directly or indirectly, with a particular consumer or household."[69] It also provides clarity for private causes of action and penalties, and notes that the CCPA "preempts local laws on the day of its enactment not enforcement."[70] The CCPA's first Amendment takes steps toward clarification, yet its full scope remains murky for now.

D. GDPR and CCPA Implementation

Like the GDPR, interpretation of the CCPA will become clearer over time after the law goes into effect. Until authorities take actions to enforce GDPR violations, and, eventually, violations of the CCPA, the scope of each of these privacy laws will remain uncertain. In the meantime, businesses are beginning to take steps—*e.g.*, GoDaddy and WHOIS.com redaction of contact information from databases for EU addresses—in conjunction with the passage of the GDPR, the CCPA, and additional existing and pending privacy laws within the United States.[71] However, the future of the CCPA is uncertain. Currently, large "companies including Amazon, AT&T, Apple, and Google are lobbying Congress to craft legislation that would preempt" the CCPA and any other state or local privacy laws within the United States.[72]

E. Adopting Privacy Law Standards in an Uncertain Time

While privacy laws appear to be trending toward giving consumers greater control over their data, it is important to note how recent laws and regulations align with and, in some cases, diverge from, one another. It appears that the use of personal information collected from consumers, particularly biometric, financial, and other sensitive data, will be subject to ever-increasing restrictions and control. However, which businesses and activities will be subject to these regulations will differ from jurisdiction to jurisdiction.

Practitioners should understand their clients' current business practices involving collection, storage, use, and sharing of personal data and how these practices may change over time. As a starting point, California business attorneys should ask the following five questions of their non-EU-based clients in assessing whether the GDPR is applicable:

1. Does your business offer any goods or services to EU residents or monitor the behavior of any individuals within the EU?
2. What languages and currencies does your website use?
3. What types of data do you collect when users access your website (e.g., IP addresses) and what types of information do users provide (e.g., name, email, address, credit card, etc.)?
4. Does your business combine the data collected or use any type of anonymization or pseudonymisation process when data is stored?
5. Does your business use any third-party data processors?

Compliance with applicable privacy laws extends beyond merely updating a company's privacy policy and identifying applicable laws and regulations. A California business attorney may need to work with their client's chief technology officer or chief information officer.

Alternatively, they may recommend that the client engage an outside consultant to ensure the company's computer network and systems that collect, process, and store data are in compliance and consistent with the company's privacy policy.

Privacy law compliance today represents an attempt to strike a moving target. Attorneys will need to stay informed of new privacy laws as lawmakers and regulators in the EU and the U.S. struggle to keep up with new data collection technologies.

Endnotes

1 Regulation (EU) 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), art. 4(1), 2016 O.J. (L 119) 1, 33 [hereinafter GDPR]; *see also* Ruth Boardman, Bird & Bird, Guide to the General Data Protection Regulation 2 (2017).

2 GDPR art. 3(2).

3 *Id.* at art. 4(2).

4 *Id.* at art. 4(7), (8).

5 Boardman, *supra* note 1, at 2.

6 GDPR art. 13(1).

7 *Id.* at art. 12(1).

8 *Id.* at recital 32; *see also id.* at art. 4(11).

9 *Id.* at recital 32.

10 *Id.* at art. 8(1).

11 *Id.* at art. 8(2).

12 *Id.* at art. 7(3).

13 *Id.* at art. 17.

14 *Id.* at art. 13(2)(b).

15 *Id.* at art. 20.

16 *Id.* at art. 12(3). The one month provision may be extended up to two months in complex cases, but the controller still must provide notice within one month of receipt of the data subject's request.

17 Boardman, *supra* note 1, at 35.

18 GDPR art. 37(1)(c); *see also id.* at art. 9(1) (stating "[p]rocessing of personal data revealing 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 shall be prohibited."); *id.* at art. 10 (discussing the "[p]rocessing of personal date relating to criminal convictions").

19 GDPR art. 37; *see also id.* at art. 39.

20 *Id.* at art. 27.

21 *Id.* at recital (39).

22 *Id.* at art. 5(1)(e).

23 *Id.* at recital (26).

24 *Id.* at art. 17(1).

25 *See id.* at art. 82, 83.

26 *Id.* at art. 51 (1); *see also* Boardman, *supra* note 1, at 54–57.

27 GDPR art. 83(5).

28 Thomas Brewster, *How Facebook Was Hacked and Why It's a Disaster for Internet Security,* Forbes (Sept. 29, 2018, 11:46 AM), https://www.forbes.com/sites/thomasbrewster/2018/09/29/how-facebook-was-hacked-and-why-its-a-disaster-for-internet-security.

29 Chris Baraniuk, *Vote Leave Data Firm Hit with First Ever GDPR Notice*, BBC (Sept. 20, 2018), https://www.bbc.com/news/technology-45589004; *see also* Info. Comm'r's Office, Enforcement Notice: The Data Protection Act 2018 Part 6, Section 149 (July 6, 2018) https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf.

30 Baraniuk, *supra* note 29.

31 *Id.;* Info. Comm'r's Office, *supra* note 29.

32 Baraniuk, *supra* note 29; Info. Comm'r's Office, *supra* note 29.

33 Info. Comm'r's Office, *supra* note xxix.; *see also* Baraniuk, *supra* note 29.

34 Rob Davies, *BA Customers' Credit Card Details 'Probably Already for Sale,'* The Guardian, (Sept. 7, 2018, 12:45 PM), https://www.theguardian.com/business/2018/sep/07/ba-british-airways-customers-hacked-credit-card-details-dark-web.

35 *Id.*

36 *Id.*

37 Phil Muncaster, *Nielsen Shareholder Sues Over GDPR Statements*, Infosecurity Mag. (Sept. 6, 2018), https://www.infosecurity-magazine.com/news/nielsen-shareholder-sues-over-gdpr.

38 *Id.*

39 *Id.*

40 Brian G. Cesaratto & Deanna L. Ballesteros, California's New Consumer Privacy Act: What Employers Need to Know (July 30, 2018), https://www.ebglaw.com/content/uploads/2018/07/Act-Now-Advisory_California-Consumer-Privacy-Act.pdf.

41 *See* 740 Ill. Comp. Stat. Ann. 14/5 (West 2008).

42 *Id.* at 14/10.

43 201 Mass. Code Regs. 17.05 (2010).

44 *Id.* at CMR 17.01(2), 17.02(3).

45 *Id.* at 17.03.

46 N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00 (2017).

47 *See id.* at 500.01–16.

48 Sasha Ingber, *Facebook Will Stop Funding Opposition to a User Privacy Initiative in California*, NPR (Apr. 12, 2018, 7:15 PM), https://www.npr.org/sections/thetwo-way/2018/04/12/602002272/facebook-will-stop-opposing-

a-user-privacy-initiative-in-california; *see also* Alastair Mactaggart, *About Us*, *Californians for Consumer Privacy,* https://www.caprivacy.org/about-us.

49 Ingber, *supra* note 48 (internal quotation marks omitted) (quoting KQED report).

50 *Id.*

51 *Id.*

52 California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 § 2(a) (A.B. 375) (West 2018) [hereinafter CCPA] (to be codified at Cal. Civ. Code §§1798.100–1798.198).

53 *Id.* at § 2(b).

54 *Id.* at § 2(g).

55 Mactaggart, *supra* note 48.

56 CCPA § 2(i).

57 *See id.*

58 *Id.* at § 3 (Cal. Civ. Code §§ 1798.100, 1798.105, 1798.110).

59 *Id.* at § 3 (Cal. Civ. Code § 1798.100(d)).

60 *Id.*

61 *Id.* at § 3 (Cal. Civ. Code § 1798.120(a)–(b)).

62 *Id.* at § 3 (Cal. Civ. Code § 1798.140(c)).

63 *Id.* at § 3 (Cal. Civ. Code § 1798.150(a)); *see* 2017 California Senate Bill No. 1121 (2017-2018 Reg. Sess.) [hereinafter SB-1121] (amending the CCPA).

64 CCPA § 3 (Cal. Civ. Code § 1798.150(a)).

65 CCPA § 3 (Cal. Civ. Code §1798.155).

66 S.B. 1121, 2017-2018 Reg. Sess. (Cal. 2018).

67 Robin B. Campbell & Shalin R. Sood, *Amendments to the California Consumer Privacy Act of 2018: Progress toward Clarity*, Nat'l L. Rev. (Sept. 26, 2018), https://www.natlawreview.com/article/amendments-to-california-consumer-privacy-act-2018-progress-toward-clarity.

68 *Id.*

69 *Id.*; S.B. 1121 § 9 (Cal. Civ. Code § 1798.140(o)).

70 Campbell & Sood, *supra* note 67.

71 Jennifer Theis, *Trademark Enforcement Implications of Europe's General Data Protection Regulation (GDPR)*, IPWatchdog.com (Sept. 11, 2018), http://www.ipwatchdog.com/2018/09/11/trademark-enforcement-implications-general-data-protection-regulation-gdpr.

72 Jessica Guynn, *Amazon, AT&T, Google Push Congress to Pass Online Privacy Bill to Preempt Stronger California Law*, USA Today (Sept. 26, 2018, 5:17 PM), https://www.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/.