ARE THE EU GDPR AND THE CALIFORNIA CCPA BECOMING THE DE FACTO GLOBAL STANDARDS FOR DATA PRIVACY AND PROTECTION?

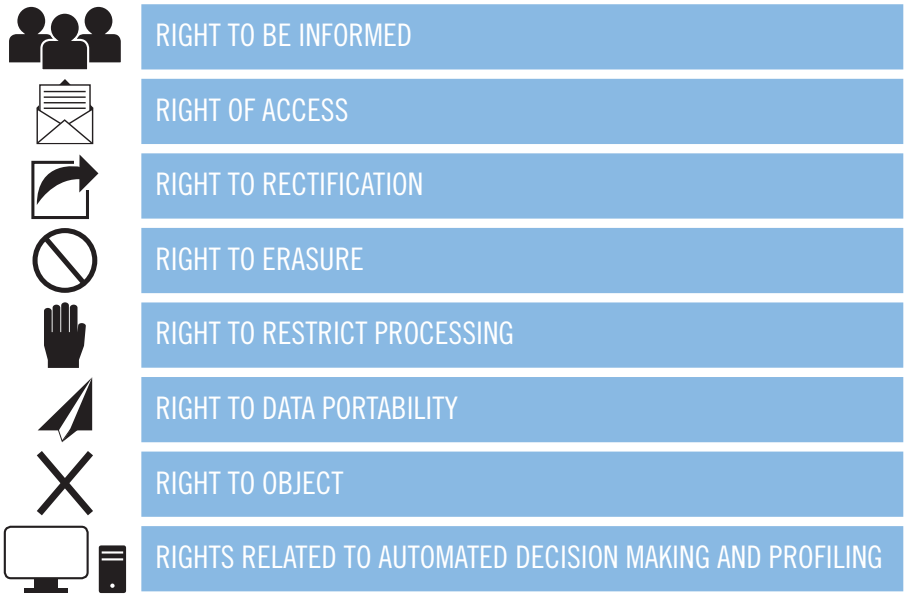
BY CATHERINE BARRETT

The GDPR is designed to protect the personal data[1] of an estimated 508 million people in the European Union (EU), the third-largest geo-political population in the world after China and India.[2] The new regulation automatically applies to all 27 member states as of May 25, 2018, and includes eight new individual rights. In addition, the GDPR imposes new requirements on organizations that process personal data and are established in the EU and, in some cases, organizations that are established exclusively outside the EU.[3] The broad application of the new regulation within the EU and the extraterritorial scope, which is articulated in Article 3, along with the possibility of hefty fines, which are detailed in Articles 83 and 84, are driving widespread adoption of the GDPR.

In the United States, there is a different approach to individual rights and data privacy protections. The culture in the U.S. is substantially different than in the EU regarding individual rights and data privacy protections. Critics of the U.S. model assert that the U.S. "has only a patchwork of sector-specific laws that fail to adequately protect data" and there is no individual right to data privacy and/or data protection enshrined in the U.S. Constitution.[4] However, the California Consumer Privacy Act (CCPA), which became law on June 28, 2018, and goes into effect January 1, 2020, is broadly applicable to American companies. According to the International Association of Privacy Professionals, more than half a million U.S. companies are likely impacted by the law. In addition, the law

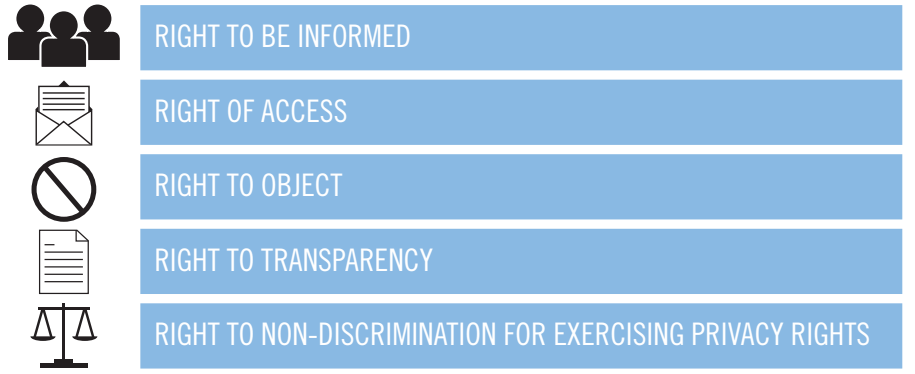
Catherine Barrett *(cabarrett@mitre.org) is a cyber policy principal with MITRE in McLean, Virginia, and co-author of What Is . . Telemedicine?, a health law primer on telemedicine published by the American Bar Association. She earned the (ISC)2 Systems Security Certified Practitioner (SSCP) certification in 2018. She received her JD and MBA from the American University Washington College of Law and Kogod School of Business, respectively.*

FIGURE 1



Source: GDPR individual rights, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights.

FIGURE 2



Source: CCPA individual rights, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=California+Consumer+Privacy+Act+of+2018.

may apply to those operating outside the U.S. too. "The fact that a business does not have a physical location in California does not exempt it from its legal obligation to comply with California law, unless every aspect of the business's commercial conduct with respect to the consumer's personal information takes place "wholly outside of California."[5] The number of businesses that potentially fall within the CCPA's scope, combined with the number of people the law is intended to protect—an estimated 39.5 million California residents—means the law is of global significance. The GDPR and CCPA are becoming the de facto global standards for data privacy and protection because of the sheer volume of citizens protected (~508 million in the EU and ~35.9 million California residents, respectively) and the wide applicability of the laws to companies. This article addresses common elements of these laws and origins of data privacy that, in an era of globalization, are likely to drive common behaviors among organizations globally.

Background

There is a cultural difference between how privacy rights and data protections

are viewed in the U.S. and how they are viewed in the EU. Europeans "operate from a perspective that customers own their data, whereas U.S. companies see themselves as owning the data because they are either the employer or the ones who spent millions (or billions) to harvest and analyze that data."[6] Generally, "privacy and data protection are two rights enshrined in the EU Treaties and in the EU Charter of Fundamental Rights."[7] The EU "has elevated data privacy into the realm of individual rights" and protected those rights via the General Data Protection Regulation (GDPR).[8]

In the United States, however, there are no such equivalent rights. Unlike the EU, in the U.S. there is no individual right to data privacy and/or data protection enshrined in the U.S. Constitution. The Fourth Amendment does not provide a "general constitutional right to privacy."[9] Rather, it protects individual privacy against certain kinds of government intrusion. The Fourth Amendment protects people from *unreasonable* searches and seizures by the government but does not a guarantee a general right to privacy. Reasonableness is determined by balancing two important interests: (1) the intrusion on an individual's Fourth Amendment rights and (2) the legitimate government interest, such as public safety.[10] For example, "searches and seizures inside a home without a warrant are presumptively unreasonable," but "if the items are in plain view" or "if the search is incident to a lawful arrest," there may be no need for a warrant.[11] Thus, in the U.S., the right to privacy is *contextually based* and limited in scope.

There are some U.S. federal laws that recognize a right to privacy and data protection outside this Fourth Amendment construct. However, these laws are generally limited in scope to specific sectors. For example, Gramm-Leach-Bliley Act applies to the financial industry and provides narrowly tailored data privacy protections under specific circumstances. Another example is the Health Insurance Portability and Accountability Act (HIPAA) that seeks to protect individually identifiable health information in any form (electronic, paper, or oral).

Nevertheless, the cultural differences between the U.S. and EU on privacy rights and data protections mean that U.S. companies may struggle to understand and implement the GDPR. The fact that U.S. citizens do not have general data privacy rights and protections enshrined in the Constitution or federal statute results in companies, at least initially, fundamentally treating data differently in the U.S. than in the EU.

GDPR Scope Is Driving Global Adoption

Article 3 – Extraterritorial Scope

According to the European Commission, there are two criteria under Article 3 for determining what entities fall within the GDPR: (1) a company or entity that processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or (2) a company established outside the EU offering goods/services (paid or for free) or monitoring the behavior of individuals in the EU. Article 3 further details that data controllers outside the EU may fall within the GDPR "if it processes data about individuals who are in the EU and processing relates to either: (1) the offering of goods or services to data subjects who are in the EU; or (2) monitoring their behavior, where that behavior takes place in the EU."[12] Examples of data controllers include Marriott International, Amazon, and Wells Fargo Bank. These companies are data controllers because they determine the purpose for collecting personal data and the means by which EU personal data are processed. A data processor is generally a third party that processes personal data on behalf of the data controller. Article 4 defines a data processor as a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. Amazon Web Services (AWS) is an example of a data processor.

Marriott International, for example, is an American company headquartered in Bethesda, Maryland, with facilities throughout Europe. Marriott falls within the GDPR scope because the company has one or more establishments in the EU and controls and processes the personal data of individuals in the EU and offers services to them. Even if a company isn't operating in the EU, however, or dealing directly with EU citizens, it may need to comply with the GDPR. "Many American companies will end up complying with GDPR" because they "are dealing with a lot of business partners that want to be GDPR compliant" and must be GDPR compliant in order to work with those partners to avoid "contaminating their pristine GDPR compliant databases with . . . non-compliant data."[13] Thus, American companies may need to comply with GDPR because they directly or indirectly control data of individuals in the EU.

Articles 83 and 84 – Hefty Fines

In addition to the widespread scope and application of the GDPR, another factor driving global compliance of the regulation is the substantial fines that can be levied under Articles 83 and 84. Fines of up to 10 million euros or 2% of annual global revenues or the higher of 20 million euros or 4% of annual global revenue can be imposed for certain breaches. Higher fines are imposed for intentional or negligent behavior. Marriott International, for example, could be the first large, multinational U.S. company to face a significant fine under the GDPR for a data breach. On November 30, 2018, Marriott International announced a massive data breach of its reservation system that exposed the personal data, such as names, passport numbers and credit card numbers, of up to 500 million customers. Marriott disclosed "hackers had access to the reservation systems of many of its hotel chains for the past four years."[14] Article 83 details the general conditions for imposing administrative fines. Under the GDPR, the American company could face fines of up to 4% of annual revenue. In 2017, Marriott International "generated approximately 22.9 billion U.S. dollars in revenue," so the fine could total US$916 million.[15]

INDIVIDUAL RIGHTS	CCPA	GDPR	ANALYSIS
Right to be informed	X	X	CCPA: A California resident has the right to request a business[28] that collects personal information about him/her disclose the sources, purpose, categories and pieces of information collected and third parties with whom the business shares information GDPR: A data subject (natural person) has a right to ask a company about what personal data (about him or her) is being processed and the rationale for such processing.
Right to object	X	X	CCPA: At any time, a consumer has the right to tell a business selling their personal information to third parties to stop (right to opt-out).[29] GDPR: Data subjects have the right to object to data processing, including direct marketing/profiling.
Right of access	X	X	CCPA: Right to request a business that collects their personal information disclose the categories and specific pieces of personal information the business has collected.[30] GDPR: A business must provide data subjects with: (1) confirmation their data is being processed; (2) access to their personal data; and (3) other supplementary information.
Right to rectification		X	GDPR: Right to have personal data rectified if it is inaccurate or incomplete.[31]
Right to erasure and withdrawal of consent	X	X	CCPA: Right to request a business delete any personal information about the consumer which the business has collected.[32] GDPR: Right to request their data be erased where: (1) personal data is no longer needed for the purpose it was collected; (2) data subject withdraws consent/objects and there are no overriding legitimate interests to continue processing; (3) personal data was unlawfully processed or must be erased to comply with a legal obligation; or (4) personal data is processed in relation to services for a child.[33]
Right to restrict data processing		X	GDPR: Data subjects have a right to restrict processing of personal data when he/she: (1) contests its accuracy; (2) objects to the processing; or (3) where processing is unlawful.[34]
Right to transparency	X		CCPA: Right to request a business disclose the categories of personal information the business collects, sells, or discloses.[35]
Right to data portability		X	GDPR: Data subjects have the right to move, copy or transfer personal data from one IT environment to another with ease.[36]
Right to object to automated processing and profiling[37]		X	GDPR: Data subjects have a right to deny being held to a decision when: (1) it is based on automated processing; and (2) it produces a legal effect or a similarly significant effect on the individual.
Right to non-discrimination for exercising privacy rights	X		CCPA: Prohibits a business from discriminating against a consumer because the consumer exercised any of the consumer's rights under the CCPA.[38]

For companies that have a physical presence in the EU, such as Marriott International, EU member state authorities can enforce the GDPR and levy fines.[16] Companies that do not have a physical presence in the EU may be required to designate a representative that is located in a member state under Article 27, to provide a physical presence. There are exceptions, however, where data processing that is deemed "occasional" and not large scale does not require a representative.[17] Finally, companies that do not have a physical representative or a designated representative may still face fines via enforcement under international law. "EU regulators rely on international law to issue fines" and "cooperation agreements between US and EU law enforcement agencies" to enforce GDPR.[18]

CCPA Scope Will Also Drive Global Adoption

Overview of the CCPA

The California Consumer Privacy Act (CCPA) became law on June 28, 2018 and goes into effect on January 1, 2020. The passage of the CCPA is significant for at least four reasons: (1) it applies to the most populous state in the U.S. with an estimated 39.5 million residents; (2) California is the world's fifth-largest economy, according to the U.S. Department of Commerce, surpassing the economies of Germany, the United Kingdom, Japan, and China; (3) California laws often serve as a model for other state legislatures; and (4) the law is the most comprehensive set of data privacy laws and individual protections in the U.S. to date. In addition, it is possible the CCPA could influence any federal legislation Congress may consider in future years.

CCPA and GDPR: Both Recognize Individual Right of Privacy

The CCPA and the GDPR recognize an individual right of privacy as a

WHEN THE REGULATION APPLIES

Your company is a small, tertiary education company operating online with an establishment based outside the EU. It targets mainly Spanish and Portuguese language universities in the EU. It offers free advice on a number of university courses and students require a username and a password to access your online material. Your company provides the said username and password once the students fill out an enrolment form.

WHEN THE REGULATION DOESN'T APPLY

Your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject to the rules of the GDPR.

Source: The European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.

fundamental right. In 1972, the California Constitution was amended to provide a right of privacy among the "inalienable" rights of all people. In Europe, "privacy and data protection are two rights enshrined in the EU Treaties and in the EU Charter of Fundamental Rights."[19] Like the GDPR, the CCPA provides many similar rights—the right to be informed, right of access, right to erasure and withdrawal of consent, and right to object. However, the CCPA does not provide as many individual rights as the GDPR—approximately four of the total eight—and it is not as expansive in terms of global applicability as the GDPR. The scope of individual rights is more limited under the CCPA and does not include the right to rectification, right to restrict data processing, right to data portability, or the right to object to automated processing and profiling (see Table 1 on page 27 for a summary of individual rights under both the CCPA and the GDPR).

Scope of CCPA, Like GDPR, Is Broad

Once the CCPA goes into effect January 1, 2020, given California's large population and economy, and the fact that "many (if not most) American companies service California consumers," companies will need to comply with the CCPA, even if the company has no physical presence in California.[20] According to the "International Association of Privacy Professionals, it is estimated that more than half a million U.S. companies will be impacted by the law, many of them small-to-mid-sized businesses."[21] The CCPA applies to "for-profit businesses that collect and control California residents' personal information, do business in the State of California, and: (a) have annual gross revenues in excess of $25 million; or (b) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or (c) derive 50% or more of their annual revenues from selling California residents' personal information. The Act also draws in corporate affiliates of such businesses that share their branding."[22] The CCPA defines "personal information" as information that identifies, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.[23]

Much like the GDPR, companies will likely comply with the CCPA rather than risk a penalty. Realistically, "few companies are likely to devote the resources necessary to provide . . . opt-out options to a user visiting a Web site from an IP address in California, while providing a Web site without those features to residents of the other 49 states."[24] There are, however, exemptions under the CCPA. A company doesn't need to comply with the CCPA "if every aspect of … commercial conduct takes place wholly outside of California," meaning that (1) the business collected the information from the consumer in question while he or she was outside California, (2) no part of any sale of his or her personal information occurred in California, and (3) no personal information collected while the consumer was in California is sold."[25] However, many companies will fall within the scope of the CCPA because California residents are among their customers.

Like GDPR, CCPA Risk of Fines Will Drive Compliance

Both the GDPR and the CCPA include an individual right to hold an organization accountable for violations of data privacy protections. Under the GDPR, a data subject has the right to lodge a complaint with a supervisory authority in his/her Member EU state of residence, workplace, or place where the violation took place.[26] A supervisory authority is established in each EU member state and is an independent governmental entity that supervises compliance with the GDPR. Supervisory authorities consider a list of criteria, such as intent and severity of the infringement, when calculating the fine. Total fines range from the high (up to 20 million euros or up to 4% of total revenues of the preceding fiscal year, whichever is higher) to the more moderate (up to 10 million euros or up to 2% of total revenues of the preceding fiscal year, whichever is higher).

Under the CCPA, a California resident may hold an organization accountable by filing a complaint with the California Attorney General (AG) or pursuing a private right of action. Consumers may pursue a private right of action if a business violates its duty to implement and maintain reasonable security procedures. A consumer may pursue a civil action: (A) To recover damages no less than one hundred dollars ($100) and no greater than seven hundred and fifty ($750) per consumer, per incident or actual damages, whichever is greater; or (B) Injunctive or declaratory relief; or (C) Any other relief the court deems proper.[27]

Conclusion

The GDPR, which is designed to protect the personal data of the more than 500 million people in the EU, and the CCPA, which is designed to protect nearly 40 million California residents, were crafted to protect individual privacy as a fundamental right. The millions of companies around the world that are complying with the GDPR and will have to comply with the CCPA mean that these laws are becoming the de facto global standards for data privacy and protection. ◆

Endnotes

1. Article 4 defines personal data to include name, an identification number, location data, physical, physiological, genetic, mental, economic, cultural, or social identity of natural person. IP addresses, cookie identifiers, mobile device ID, and other types of online identifiers are also considered personal data.

2. *Living in the EU, Size and Population*, EU (Feb. 2, 2018), https://europa.eu/european-union/about-eu/figures/living_en (last visited Dec. 18, 2018).

3. Allen & Overy, LLP, Preparing for the General Data Protection Regulation (Jan. 2018), http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

4. *Council on Foreign Relations, Reforming the U.S. Approach to Data Protection and Privacy* (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

5. Melissa A. Kern, et al., *Does the New California Privacy Law Apply to Your Business?* Frost, Brown, Todd, LLC, July 19, 2018, https://www.frostbrowntodd.com/resources-2182.html.

6. Dan Seyer, *Does GDPR Matter to Your U.S. Company, Customers, Partners or Ecosystem?* Forbes Mag. (June 13, 2018), https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/13/does-gdpr-matter-to-your-u-s-company-customers-partners-or-ecosystem/#2d5da80965f4.

7. EU, European Data Protection Supervisor, *Data Protection*, https://edps.europa.eu/data-protection_en (last visited Dec. 12, 2018).

8. P. Berman, *GDPR in the U.S.: Be Careful What You Wish For*, Gov't Tech. Mag. (May 23, 2018), *available at* http://www.govtech.com/analysis/GDPR-in-the-US-Be-Careful-What-You-Wish-For.html.

9. Katz v. United States, 389 U.S. 347, 350 (1967). *See also* Catherine M. Barrett, *FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy*, 8 Rich. J.L. & Tech. 16 (2002), *available at* http://scholarship.richmond.edu/jolt/vol8/iss3/3.

10. *What Does the Fourth Amendment Mean?* U.S. Courts, http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (last visited Dec. 18, 2018).

11. *Id.*, *See also* Payton v. New York, 445 U.S. 573 (1980) (searches and seizures inside a home without a warrant are presumptively unreasonable); United States v. Robinson, 414 U.S. 218 (1973) (if the search is incident to a lawful arrest); and Maryland v. Macon, 472 U.S. 463 (1985) (if the items are in plain view).

12. Allen & Overy, LLP, *supra* note 3.

13. Seyer, *supra* note 6.

14. Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting Up to 500 Million Guests*, Washing. Post (Nov. 30, 2018), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?utm_term=.b4048d495d06.

15. *Living in the EU*, *supra* note 2.

16. Aaron W. Winston, *How the EU Can Fine US Companies for Violating GDPR*, Spiceworks.com (Oct. 2, 2017), https://community.spiceworks.com/topic/2007530-how-the-eu-can-fine-us-companies-for-violating-gdpr.

17. Article 27 details exceptions to data processing.

18. Winston, *supra* note 16.

19. Data Protection, *supra* note 7.

20. Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, Proskauer Privacy Law Blog (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018.

21. Kern, et al., *supra* note 5.

22. Mathews & Bowman, *supra* note 20.

23. For more details, *see* Bill No. 375, Sec. 3, tit. 1.81.5, § 1798.140.

24. Mathews & Bowman, *supra* note 20.

25. *Id.*

26. Art. 77, Right to lodge a complaint with a supervisory authority.

27. Bill No. 375, Sec. 3. tit. 1.81.5, § 1798.150.

28. Bill No. 375, Sec. 3. tit. 1.81.5, § 1798.110. "Business" is as a sole proprietorship, partnership, limited liability company, corporation, association or other legal entity, operated for the profit or financial benefit of its owners, alone or with others determines the purposes and means of the processing of commercial information of products or services purchased, or of purchasing or consumer histories or tendencies, does business in the state of California; and meets *one or more* of the following three thresholds: (1) Has annual gross revenues exceeding $25,000,000; (2) Annually buys, receives, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; and (3) Derives 50% or more of its annual revenues from selling consumers' personal information.

29. Bill No. 375, Sec. 3. tit. § 1.81.5, 1798.120.

30. Bill No. 375, Sec. 3. tit. § 1.81.5, 1798.100.

31. Article 16 provides the right to rectification. Art. 19 details the notification obligation regarding rectification or erasure of personal data or restriction of processing.

32. Bill No. 375, Sec. 3. tit. 1.81.5, § 1798.105.

33. Article 17 details the right to erasure. *See also* McCallum, Patrick, Id.

34. Article 18 details the right to restriction of processing.

35. Bill No. 375, Sec. 3. tit. 1.81.5, § 1798.115.

36. Article 20 details the right to data portability.

37. Article 4 defines "profiling" as any form of automated processing of personal data . . . to analyze/predict aspects of that person's performance at work, economic situation, health, etc.

38. Bill No. 375, Sec. 3. tit. 1.81.5, § 1798.125.