



Privacy Basics for Colorado Lawyers

The Colorado Consumer Data Privacy Act
and the California Consumer Privacy Act

BY JENIFER MCINTOSH

In this world of ever-proliferating acronyms, it can be difficult to determine which ones to pay attention to, particularly in the legal community, and even more so when working with clients in technology. Most of us know what HIPAA, USPTO, and COPPA stand for and what effect they have, if any, on our particular practice areas. But public outcry and growing privacy concerns have spawned two significant laws that may not be on every Colorado attorney's radar: California's looming Consumer Privacy Act¹ (CCPA²), and Colorado's recently enacted Consumer Data Privacy Act³ (CDPA⁴). Many of our clients—large and small—have casually shrugged off any privacy compliance or assessment efforts regarding exposure under the EU's General Data Protection Regulation

(GDPR), and some rightfully so, given the lack of customers, marketing, or presence in the EU or European Economic Areas. The CCPA and CDPA, however, hit closer to home, and will likely have an impact—wanted or not. While this article focuses on the basic provisions of Colorado's lesser-known CDPA, it also discusses how California's legislation will impact Colorado lawyers when it goes into effect January 1, 2020.⁵

CDPA: The Brass Tacks

The CDPA became effective on September 1, 2018, and requires entities collecting or monetizing data to use reasonable and appropriate measures to protect Colorado residents' "personally identifiable information" (PII). The law has two basic components. The first part

governs how "covered entities" safeguard the PII they maintain, own, or license. The second part governs when those entities must report a breach of "personal information" (PI) to the respective Colorado residents, including when and what they must disclose when such a breach has occurred.

If your client is a person, commercial entity, or governmental entity that collects, uses, licenses, or owns information gathered from Colorado residents, your client has a statutory responsibility to protect this personal information *and* to report any breach of the data collected.⁶ One quirk in Colorado's data breach law is that covered entities have an obligation to protect all information, whether in hard copy or electronic form. However, when a breach of said information occurs, the entity only has to disclose the breach of unencrypted, *computerized* PI, which is different and separate from PII.⁷

The CDPA defines PII, for security purposes, as

- a social security number,
- a personal ID number,
- a password or pass code,
- a government and/or state-issued ID number,
- a passport number,
- biometric data,
- an employer, student, or military ID number, or
- financial transaction device information (credit card number, etc.).⁸

Under the data security portion of the CDPA, companies must develop written policies documenting their destruction policy for both written and electronic PII records.⁹ This part of the law also requires covered entities to have "reasonable security procedures and practices," appropriate to the nature of the PII and the nature and size of the business, to protect the PII collected, used, or both.¹⁰ Covered entities are required to make sure third-party service providers also comply with the CDPA and employ these same protective measures.¹¹ This means if your client CrossGym owns a workout app that collects activity and health data, and CrossGym uses a third party to store the data it is collecting and analyzing, CrossGym is ultimately

responsible to the Colorado government and to Colorado citizens for the security of that data, regardless of who has it or where it is stored (yes, there is a flourishing cybersecurity insurance industry).

Although the law also requires CrossGym to create and implement policies ensuring the PII is destroyed when it is no longer needed, it does not appear necessary for CrossGym to also require the same of its third-party vendor. However, the third-party vendor, as one who “maintains” the PII of Colorado residents on behalf of a covered entity, will have to comply with the CDPA requirements as well.

PI (again, separate from PII), for purposes of the breach notification obligations of the CDPA, includes a separate and unique combination of information. A breach of PI that is *neither encrypted nor redacted* occurs when there is an unauthorized taking of

1. the first name or first initial and last name of the Colorado resident, plus one of the following:
 - social security number,
 - employer, student, or military ID number,
 - passport number,
 - driver’s license or government/state-issued ID number,
 - medical information,
 - biometric data,
 - health insurance ID number; or
2. the username or email with password/security question (with answer); or
3. the account number or credit/debit card number with security code, access code, or password.¹²

An unauthorized acquisition of unencrypted, computerized PI is a “security breach” under the CDPA.¹³ Investigation of any such breach must be prompt and performed in good faith.¹⁴ If an investigation determines no misuse occurred or is not “reasonably likely” to occur, notice of the breach is not required.¹⁵ If your investigation, however, determines the opposite is true, notice must be given to those whose data was affected and must occur no later than 30 days after it has been determined the data breach occurred. One way to help a client avoid some (but not all) breach issues is to encrypt the data. If a breach

occurs and the client’s data is encrypted, you’ve saved yourselves some long-term heartburn.

When 500 or more Colorado residents are affected by a security breach, the entity must also notify the Colorado Attorney General.¹⁶ If the number affected is 1,000 or more, notification must be provided to the consumer reporting agencies that compile and maintain files on consumers (e.g., Equifax).¹⁷ Specific information is required for all notices, and guidelines exist for how to provide such notices. In general, notice needs to be made in a realistic manner that is reasonably likely to fully inform the affected Colorado resident, as well as reach that Colorado resident.¹⁸ For instance, if the email account of a resident has been breached, notice needs to be sent via a different, reliable medium other than that breached email account. Clients who are governed by a separate legal notice requirement (such as HIPAA’s 45-day requirement) need to review their breach notification policies. The Colorado Attorney General’s office has made clear that notice of a breach of Colorado residents’ PI must be given within 30 days, regardless of what other laws’ guidelines may demand.

Coordinating CCPA and CDPA Requirements

The CCPA, unlike Colorado’s law, is not yet in effect. When it does come knocking in January 2020, the law will usher in a new state of being for entities collecting consumer data, whether or not they sit in California. While you might initially believe the CCPA is unlikely to affect your clients, consider just how large the economy of California is¹⁹ and the fact that 6.9% of the U.S. GDP in 2017 was driven by the digital economy.²⁰

Generally, a company—including one in Colorado—will have to comply with the CCPA if it takes in personal information about California residents and meets one of the following criteria:

- It has annual revenues of at least \$25 million.
- It obtains personal information from at least 50,000 California residents, households, or devices. (This includes collection of IP addresses from websites or the use of cookies to collect information on 50,000 or more California residents or devices,

including cell phones, tablets, or other IoT devices.²¹ This works out to about 138 data points a day.)

- It receives more than 50% of its revenue from selling personal information about California residents.²²

If the CCPA applies, it will—like the CDPA—require the client to have “reasonable security” measures to protect data collected on California residents, including employee²³ information. This becomes especially important under the CCPA, since both the California Attorney General and California residents will be able to sue when a company fails to employ reasonable security measures to protect their data. Data is now a valuable commodity, and a larger part of our economy than most people realize.²⁴

The major difference between the CDPA and the CCPA is the additional rights provided to consumers under the CCPA, including requests for deletion and (most frightening to clients) a private right of action when lack of reasonable security results in the “unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information.”²⁵

Personal information under the CCPA is also more broadly defined than in the CDPA. CCPA “PI” also includes inferences that can be drawn from personal information (such as preferences, behavior, intelligence), and further includes “[i]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” Similar to Colorado’s law, the California Attorney General has the right to investigate and enforce the CCPA.²⁶ If proven, a violation can lead to a \$2,500 fine per violation, or up to \$7,500 per violation if such violations are intentional.²⁷


In addition, exceptions with regard to who and what the CCPA covers are broader than those under the CDPA. The CCPA, for example, does not apply to nonprofits, period.²⁸ With regard to entities regulated by HIPAA, the Gramm-Leach-Bliley Act, or the Fair Credit Reporting Act (FCRA), information collected pursuant to those is not subject to the CCPA. We will have to wait and see if further gaping holes and theft

of sensitive consumer data from entities such as Equifax,²⁹ Employees Retirement System of Texas,³⁰ and Wells Fargo³¹ have any effect on the FCRA exceptions or others under the CCPA, despite what are likely furious lobbying efforts of these industries.

In contrast to the CCPA, the CDPA does not explicitly exempt certain sectors from the law's application. While the Colorado Attorney General has noted that compliance with other privacy regulations is generally sufficient,³² where the CDPA rules establish additional or more rigorous requirements than other regulations, compliance with the CDPA rules is required notwithstanding (e.g., the 30-day notice requirement under CDPA applies even though HIPAA requires notice within 45 days).

Conclusion

So, what do these new regulations require of the attorney not wholly immersed in privacy or cyber security law? At the bare minimum, they require you to find out if your clients collect, maintain, buy, own, or use data, how much, and where and how it is stored. Generally speaking, if your clients maintain Colorado employee or customer information, the CDPA applies to your clients and the data they hold. The client must take "reasonable security" measures to protect the information, have a written policy for maintaining and destroying the information, and comply with set timing and content protocols for assessing and reporting a breach of that information.

If your clients receive and solicit a substantial amount of business from California, or derive a large part of their income from the collection, analysis, or sale of data, you will need to ask more questions to determine how close they are to falling under the CCPA. A good information security officer, if the company doesn't have a privacy officer, should know where to start in an assessment. If not, don't despair; Colorado is full of knowledgeable, practically minded privacy attorneys who can help. 

A version of this article was first published in the University of Denver Sturm College of Law Online Supplement to the Denver Law Review, in May 2018.



Jenifer McIntosh is a data privacy and intellectual property attorney at Thomas P. Howard LLC in Louisville, Colorado. Her practice includes transactional and litigation matters involving privacy compliance, patents, trade secrets, trademarks, copyrights, and anything data related (including use of data in hemp-related businesses). She is a Baylor Law alumna, a former EDTX federal law clerk, and a First and Fourth Amendment junkie.

Coordinating Editor: Joel Jacobson, joel@rubiconlaw.com

NOTES

1. The CCPA is effective January 1, 2020. However, the law includes a 12-month "look back" period, allowing consumers to request disclosure of their PI kept for up to one year before the actual request. California Consumer Privacy Act of 2018, Cal Civ. Code Div. 3, Pt. 4, Tit. 1.81.5 (operative Jan. 1, 2020).
2. California Legislative Information, AB-375 Privacy: personal information: businesses, https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375.
3. HB 18-1128, 71st Gen. Assemb., Reg. Sess. (Colo. 2018) (enacted).
4. The Colorado Consumer Data Privacy Act is not widely known by the acronym "CDPA," but this acronym is used in this article for the sake of convenience.
5. While the CCPA will become effective January 1, 2020, amendments passed on August 31, 2018 delay the California Attorney General's ability to enforce the law by six months after the AG's office publishes its implementing regulations or July 1, 2020, whichever is first. CCPA § 1798.185(a).
6. CRS § 6-1-713.5, 716.
7. CRS § 6-1-716.
8. CRS § 6-1-713(2)(b).
9. CRS § 6-1-713(1).
10. CRS § 6-1-713.5(1).
11. CRS § 6-1-713.5(2).
12. CRS § 24-73-103(g)(1)(A) to (C).
13. CRS § 6-1-716(1)(h).
14. CRS § 6-1-716(2).
15. *Id.*
16. CRS § 6-1-716(2)(f).
17. *Id.*
18. Colorado's Consumer Data Protection Laws: FAQ's for Businesses and Government Agencies, Colorado Attorney General, <https://coag.gov/resources/data-protection-laws>.
19. California has the fifth largest economy in the world. See "California Must Be Doing Something Right in Trump's America," Bloomberg Opinion (May 29, 2018), www.bloomberg.com/opinion/articles/2018-05-29/trump-vs-california-state-s-economy-vastly-outpaces-u-s.
20. U.S. Bureau of Economic Analysis, "Measuring the Digital Economy: An Update Incorporating Data from the 2018 Comprehensive Update of the Industry

Economic Accounts (2019)," <https://www.bea.gov/media/5481>.

21. The definition of "devices" and "households" is still unclear and likely will be defined by regulations coming out of the California AG's office prior to July 1, 2020.

22. Don't conflate the \$25 million in revenue requirement with the 50% of revenue requirement. If your client is one of those hip, open-workspace programmatic sales companies in Boulder, the CCPA applies to them. Clark Hill PCL, "California Consumer Privacy Act: Action Required by New Privacy Law," *JDSupra* (Feb. 12, 2019), <https://www.jdsupra.com/legalnews/california-consumer-privacy-act-action-91377>.

23. AB-25 to the CCPA of 2018, which was passed by the Assembly but now waits in committee or on the Senate floor, would amend Cal. Civ. Code § 1798.140(g)(2) to clarify that the definition of "consumer" does not include employees, agents of a business or contractors, or job applicants, provided the person's PI is collected and used by the business solely in that context.

24. Mandel, "The Data Economy is Much, Much Bigger Than You (and the Government) Think," *Atlantic* (July 25, 2013), <https://www.theatlantic.com/business/archive/2013/07/the-data-economy-is-much-much-bigger-than-you-and-the-government-think/278113>.

25. Stephens, "California Consumer Privacy Act," American Bar Association (Mar. 8, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9.

26. Cal. Civ. Code § 1798.155 (2019).

27. *Id.*

28. Cal. Civ. Code § 1798.140 (2019).

29. Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach, U.S. Government Accountability Office (Aug. 30, 2018), <https://www.gao.gov/products/D19401>.

30. "Largest Healthcare Data Breaches of 2018," *HIPPA J.* (Dec. 27, 2018), <https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018>.

31. Whittaker, "Millions of Bank Loan and Mortgage Documents have Leaked Online," *TechCrunch*, <https://techcrunch.com/2019/01/23/financial-files>.

32. Colorado's Consumer Data Protection Laws: FAQ's for Businesses and Government Agencies, *supra* note 18.