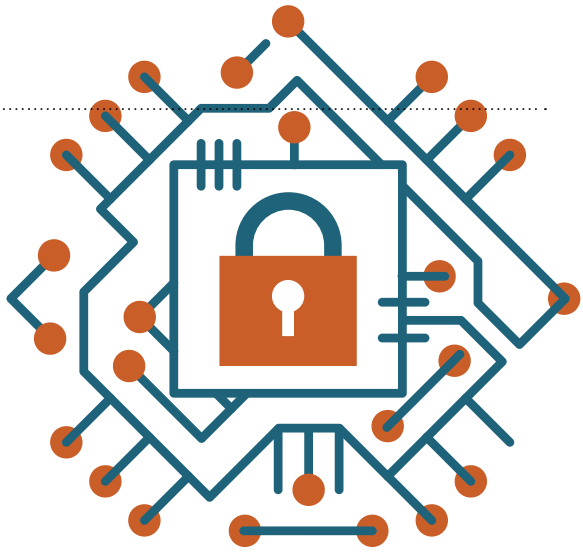

Colorado Compliance for Privacy and Security Laws from Other Jurisdictions

BY THOMAS CODEVILLA

Numbed by the constant stream of privacy law news, Colorado companies without out-of-state locations may be tempted to think privacy laws from other jurisdictions do not apply to them. Similarly, counsel for those companies may miss the nuances of laws like the General Data Privacy Regulation (GDPR), California Consumer Privacy Act (CCPA), Children's Online Privacy Protection Act (COPPA), or Video Privacy Protection Act (VPPA) that compel their seemingly exempt clients to comply.

To further complicate matters, many privacy laws require information "security" without defining the term, partly because reasonable security is organization-specific and partly because lawyers discussing cybersecurity sound like your grandparents trying to explain the Internet. Luckily, security organizations and professionals have begun to fill in the gap.

What follows is an exploration of the several ways privacy laws from other jurisdictions can apply to Colorado businesses and how those businesses can approach the concept of "reasonable" security.

A Security and Applicability Cheat Sheet for General Practitioners

The Appendix contains a chart with several issue-spotting tools for generalists who might think their Colorado-only clients are exempt from the provisions of the GDPR, CCPA, COPPA, or VPPA. As a refresher: the GDPR governs the collection and use of personal data from EU data subjects; the CCPA governs the collection and use of personal information from California consumers; COPPA sets rules for the collection of personal information online from children under 13 in the United States; and the VPPA protects individuals' video viewing history. As the chart shows, the laws provide little guidance on required security; the second part of this article attempts to fill that gap.

The chart highlights two themes in privacy law. First, collecting information online usually subjects a company to some kind of regulation, meaning that companies seeking to shrink their compliance footprint should first catalog their data collection, use, sharing, and retention in a practice known as "data mapping." Without a comprehensive data map, it is impossible to begin privacy law compliance and nearly impossible to secure a business's data.

The second theme is that privacy laws are terrible at spelling out security requirements for the data the laws purport to protect. So, what might reasonable security look like?

Practical Security for Privacy Law Compliance

Suppose your client must comply with one of the above laws and asks how to secure its data. How would you proceed beyond imploring the client's IT staff to explain their jobs to you?

First, there is a separate but increasingly parallel world of security policy. Organizations like the National Institute of Standards and Technology (NIST) and the International Organization for Standards (ISO) have created detailed standards for security, complete with best practices.[1] My conversations with regulators have indicated that implementing NIST or ISO standards might inspire some regulatory lenience in case of a data breach. Both standards contain practical guides to securing your organization's data in layman-accessible language. Familiarize yourself with NIST and ISO requirements and then buy the IT department lunch; you will be shocked at how much you learn.

Second, on your IT "front end," update your privacy policies and contracts to reflect your commitment to security:

- As mentioned above, map your data to ensure you have a comprehensive view of your organization's practices.
- Revise your privacy policy to include your new security procedures and breach response protocols.
- Update your terms of service to specify age limits for your users, your rights to use the data collected, and a process for handling disputes.
- Amend contracts with third party vendors handling data to ensure they store your data securely and only use it as you instruct.
- Vendors handling sensitive information should sign a comprehensive data processing agreement (DPA) containing an increased commitment to security, assisting with consumer rights requests, and breach reporting.

Third, on the back end, there are some basic security protocols that companies of any size can implement:

- Create information security, data retention/deletion, and incident response plans, then train relevant staff periodically on how to implement each policy.

- Perform penetration testing on all networks at least once a year or before the roll-out of any new Internet-connected service or product.
- Encrypt all personal information in transit and at rest.
- Anonymize data whenever possible; though a recent study argued[2] that it is possible to re-identify many data points using just a few external data points, privacy law has not caught up to technology in that respect.
- Regularly delete server logs—once every 60 days if possible.
- Obtain cyber errors and omissions insurance. Pay close attention to the policy requirements around auditing and security standards, and make sure that a cyberattack via social engineering is not outside the scope of coverage.

Finally, call a privacy attorney if your client meets any of the following (decidedly non-exhaustive) criteria:

- collects data on anything people argue about over the dinner table (e.g., finances, health, sex, politics, age, or identity);
- does not have a data map;
- wants to offer goods or services in Europe, California, Nevada, or New York;
- wants to monetize customer information, even if "it's all going to be anonymized";
- has a general audience website hosting content that may be attractive to kids;
- sells Internet-connected products or services for use in schools;
- uses information about people's video viewing history, including YouTube; or
- makes an IoT (Internet of Things) product.

Conclusion

It has become difficult for Colorado companies to evade the reach of broadly drafted privacy laws from other jurisdictions. The patchwork of state privacy laws grows daily. However, with a current data map and a good news feed subscription, it is possible to issue-spot on the fly for your clients. The definition of reasonable security remains a legal grey area for most privacy laws, but a wealth of information and security standards is starting to make its way into the lawmaking process. Security standards evolve more quickly than privacy law, however, so the shelf life of compliance is measured in days or weeks, not years. Keep abreast of developments in security by subscribing to Krebs on Security, CSO Online, or The Register.

Remember, Colorado has a wealth of local privacy and security attorneys to aid less specialized practitioners. An ounce of preventative security is worth millions of dollars in breach.[3] CL

Thomas Codevilla is a partner at SK&S Law Group, where he specializes in data privacy and cybersecurity matters. He enjoys building risk-based compliance systems for emerging and growth stage companies—codevilla@skandslegal.com.

Coordinating Editor: Joel Jacobson, joel@ rubiconlaw.com

NOTES

1. *See* NIST Special Publication 800-53, https://nvd.nist.gov/800-53, and ISO's 27001 security standard, https://www.iso.org/isoiec-27001-information-security.html.

2. Imperial College of London, "Anonymizing personal data 'not enough to protect privacy,' shows new study" (July 23, 2019), http://bit.ly/363Lj5y.

3. A 2018 Forbes article cited the United States as having the highest average cost per data breach at $7.91 million. McCarthy, "The Average Cost Of A Data Breach Is Highest In The U.S." (July 13, 2018), https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#52ce76ba2f37. IBM put the average cost of a data breach in the United States in 2019 at $8.19 million. *See* https://www.ibm.com/security/data-breach.

APPENDIX
Cheat Sheet: Privacy Laws Applicable to Colorado Businesses

LAW	APPLICABILITY	PROTECTED INFORMATION	COLORADO BUSINESSES SHOULD WATCH FOR:	SECURITY REQUIREMENT
GDPR (E.U. 2018)	Applies to entities not established in the EU that process EU data subjects' personal data in connection with offering goods or services in the EU, or monitor their behavior.[1]	Personal data, meaning any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[2]	Do you ship product to Europe or run ads there? Does your app use geolocation data and/or have accounts? Are you providing services to any EU companies that involve you processing personal information? Does your website place tracking cookies on all visitors?	"[A]ppropriate technical and organizational measures to ensure a level of security appropriate to the risk . . ."[3]
CCPA (CA 2020)	Applies to any for-profit entity doing business in California that meets one of the following criteria: ▪ has revenue greater than $25 million; ▪ annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes; or ▪ derives 50% or more of its annual revenues from selling consumers' personal information.[4]	Personal information, which 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."[5]	By this point, most people know that "sell" under CCPA means any exchange for "valuable consideration." But many have overlooked the "devices" language. How many visitors did your website have last year? How many cookies does it place in a day? And do you know if even one of them was from California? It is easier to get to 50,000 devices than you might think.	No explicit data security requirement. However, there is a private right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk. The former California attorney general also released an attempt to define "reasonable" security in her 2012–15 data breach report.[6]
COPPA (U.S. 1998)	Applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children.[7]	Personal information, including name, address, online contact information, screen name, phone number, social security number, "persistent identifiers" including cookies, media containing the child's voice or image, geolocation information down to city level, and any information on the child combined with the foregoing.	In addition to services that target children explicitly, the FTC recently suggested[8] that general audience websites hosting content attractive to children could no longer ignore users that were likely children. Likely targets include video sites, all-ages games, social media services, instructional sites, forums, and most other fun things on the Internet.	Operators must "maintain the confidentiality, security, and integrity of information they collect from children . . . [and] use reasonable means, such as periodic monitoring, to confirm that any service providers or third parties with which you share children's personal information maintain the confidentiality and security of that information."[9]

LAW	APPLICABILITY	PROTECTED INFORMATION	COLORADO BUSINESSES SHOULD WATCH FOR:	SECURITY REQUIREMENT
VPPA (U.S. 1988)	Protects individuals' video viewing history by prohibiting video tape service providers from knowingly disclosing a consumer's "personally identifiable information" to third parties without his or her consent.[10] "Video tape service provider" includes "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of . . . similar audio visual materials."[11]	Personally identifiable information, including "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[12]	Anyone with access to video viewing history from a website, which could be embedded in a cookie or a user profile, is considered a video tape service provider.	A covered entity must "destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected."[13]
Consumer Data Privacy Act (CO 2018)	Requires businesses and government entities that keep either paper or electronic documents containing Coloradans' personal identifying information (PII) to use reasonable and appropriate measures to protect that PII.[14]	PII includes: social security number; personal ID number; password or passcode; government and/or state-issued ID number; passport number; biometric data; employer, student, or military ID number; and financial transaction device information.[15]	Most Colorado practitioners know that the CDPA requires a data destruction plan,[16] but a destruction plan is only part of the puzzle. Two other essential plans are an information security policy and an incident response plan. This way, organizations have comprehensive plans for collection, use, and sharing to destruction or breach of PII.	"[R]easonable security procedures and practices," appropriate to the nature of the PII and the nature and size of the business.[17]

NOTES

1. GDPR Article 3; Practice Note, Determining the Applicability of the GDPR (W-003-8899).
2. GDPR Article 4(1).
3. GDPR Article 3.
4. Cal. Civ. Code § 1798.140(c). Note that all of the applicability triggers for the CCPA could apply to a Colorado business with no physical presence in California.
5. Cal. Civ. Code § 1798.140.
6. Harris, California Data Breach Report 2012–2015 (Feb. 2016), https://src.bna.com/cFY.
7. Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions.
8. FTC Seeks Comments on Children's Online Privacy Protection Act, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule.
9. Complying with COPPA, *supra* note 7.
10. 18 USC § 2710(a).
11. 18 USC § 2710(a)(4).
12. 18 USC § 2710(a)(3).
13. 18 USC § 2710(e).
14. CRS §§ 6-1-713 et seq.
15. CRS § 6-1-713(2)(b).
16. CRS § 6-1-713(1).
17. CRS § 6-1-713.5(1).