CyberInsecurity
NOVEMBER 2018

INTERVIEW: KIRKE SNYDER / CHORUS CONSULTING LLC

THE STATE DATA PRIVACY LAW NOW IN EFFECT: COLORADO'S

All the attention may have been on Europe and California, but lawyers need to help their companies focus on the state law that's on the books.

Privacy legislation has gotten lots of attention this year. The EU's General Data Protection Regulation made the biggest splash, but California's Consumer Privacy Act followed with a powerful statement from the state where many of the big tech companies are based. Lost in the frenzy was a law that not only passed in Colorado before California's law did, but went into effect in September whereas California's law won't take effect until 2020. Colorado's law affects all companies that receive, collect, create or save personally identifiable information(PII) from Colorado residents.

***Kirke Snyder**, a practice leader at Chorus Consulting LLC in Denver, has spent much of his legal career focused on information governance, beginning when he earned a master's degree in legal administration. Suddenly his specialty of 25 years is very hot, and he's in a prime position to tell in-house lawyers that it's time they spoke up to help their companies mitigate serious compliance risks.*

***CyberInsecurity:** Has information governance ever been bigger than it is right now?*
Kirke Snyder: To illustrate the growth in this area of the law, I have documented that today every law firm in the Am Law 100 has at least one or two lawyers listed as data privacy and security specialists. I estimate that two years ago, only 90 percent of these firms would have listed this as a practice area, and five years ago, the majority of these firms had no such listing at all.

***CI:** When was the Colorado Protections for Consumers Data Privacy Act adopted, and what were the issues that the Legislature grappled with along the way?*
KS: The law (https://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_signed.pdf) was unanimously approved on May 29. What's interesting is that the bill's primary sponsor was a Republican, Cole West, who wanted to protect Colorado consumers and reduce the risk of identity theft. A number of businesses, both large and small, were concerned that the increased regulations were unnecessary and overreaching. The law applies to all entities that receive, collect, create or save PII from Colorado residents, customers, employees or even prospective employees. After the Equifax data breach in 2017, which exposed the PII of about 150 million of their customers, Colorado consumer rights groups felt that data security was a key issue that had to be addressed. Pro-business advocates argued that some of the heightened requirements were already obligatory under federal law, and that the proposed requirement to notify the attorney general in case of a data breach within seven days, which was the original proposed time frame, was not sufficient to determine if misuse of data had occurred. The bill was ultimately rewritten to give businesses more time.

***CI:** What are the law's basic requirements?*
KS: The law requires businesses of all sizes, as well as government agencies, to have a written policy explaining how

they will dispose of PII, whether in electronic or hard copy format, and the protocols through which they will implement this policy. And, if a data breach is detected, entities must alert consumers within 30 days that their data has been compromised. If more than 500 Coloradans are impacted, the entity must alert the attorney general's office. Finally, entities must take "reasonable" steps to protect the PII that they keep.

***CI:** What is the definition of "reasonable" under the law?*
KS: The Colorado law does not specifically define the "reasonable" steps that entities must take. The standard was intended to be flexible, because businesses of different sizes keep different kinds of data that may require more or less protection.

***CI:** Do you have a problem with that?*
KS: I think that it's an appropriate standard. In the law of negligence, the "reasonable person" standard is the standard of care that a reasonably prudent person would observe under a given set of circumstances.

***CI:** What are the key components of a company's reasonable security program?*
KS: Ultimately, the organization's senior management will need to convince the Colorado attorney general that what they have done is reasonable. I would advise that there are proactive tasks that must be completed to minimize or avoid liability. See page 4 of this document for a list I've prepared with my six recommendations.

***CI:** What about when a data breach occurs? What steps does the law say that a company should take then?*
KS: In the event of a breach or disclosure of PII involving Colorado residents, notice must be provided to affected residents within 30 days of discovery—without exception, which distinguishes Colorado's law from those of some other states. The information must include the estimated date of the breach and a description of the PII believed to have been acquired. The breached entity must also include its contact information, along with contacts for consumer reporting agencies and the Federal Trade Commission. The entity must also direct affected individuals to promptly change any passwords and other security information that has been stolen and could be used to access their accounts with other entities.

***CI:** What role should a company's in-house lawyers play in this process?*
KS: From my experience, 90 percent of companies large enough to have in-house counsel are probably not in compliance with this law today. And I suspect that smaller businesses without full-time legal counsel are at even greater risk, because they don't know what they don't know. Companies look to their legal departments to keep them legal. But too often in-house lawyers assume a support role

From my experience, 90 percent of companies large enough to have in-house counsel are probably not in compliance with this law today.

to the business leaders. These new data privacy laws can open the door to both civil and criminal liability. They are no joke. Lawyers need to drive the bus and bring the IT and HR departments to the table with the key business leaders to bring their companies into compliance.

The HR department could be sitting on a stack of old resumés—in electronic and hard copy formats—from job candidates who were never hired. HR could be retaining personnel files of employees who are no longer with the organization. The new Colorado law requires that organizations redact or destroy any documents with obsolete or unnecessary PII of Colorado residents. In-house lawyers must educate management on the new laws, evaluate the landscape of data containing PII, and play an active role in transforming the organization's information governance policies, practices and procedures.

***CI:** What advice do you give your clients who are wondering what they need to do?*
KS: Before I offer advice, I want to learn about the client's current practices and philosophy on information governance. For example, do they want to maintain multiple standards and protocols for each state's residents, or do they want to create a program that combines the most restrictive requirements from all states? I want to confirm where they receive, collect, create, save and sell personal information. I want to interview the IT, HR, marketing, sales, and legal representatives. Based on what they tell me, I recommend a compliance program that addresses the legal and regulatory requirements for their specific situation.

***CI:** Some lawyers are calling the new Colorado law "landmark." Is it?*
KS: It's considered landmark because it's the first comprehensive state law in effect that deals with the protection of consumer and employee PII; it has the shortest time frame within which to provide notification of a data breach in the United States; and it applies to all businesses and government entities, from one-person operations to multinational corporations.

***CI:** Compare the Colorado Consumer Data Privacy Act with the California Consumer Privacy Act.*
KS: At the highest level, the Colorado law went into effect on Sept. 1, but the California law, which was passed on June 28, doesn't begin until Jan. 1, 2020. As its name implies, the California law is about consumer data protection that targets large, for-profit e-commerce companies with gross sales in excess of $25 million. Whereas the Colorado law applies to any business or government entity's employee and customer data.

CI: *What are some big differences between these laws and the GDPR?*
KS: The California law and the GDPR have many similarities regarding subject access rights, data portability, transparency and data

security. The GDPR contains several important requirements that are missing from California's law: notably, a foreign company registration requirement; requirements for a data protection officer and impact assessments; 72-hour breach notifications; and restrictions on data transfers between countries. It also requires companies to give consumers the choice of opting in to sharing their PII. The California law, on the other hand, requires only that companies give consumers the ability to opt out of sharing their PII.

These new data privacy laws can open the door to both civil and criminal liability. They are no joke.

The Colorado law is focused primarily on encouraging companies to maintain reasonable efforts to protect personal information, to give timely data breach notifications and to destroy unnecessary personal information. Unlike the other two laws, it does not spell out monetary penalties for noncompliance. The attorney general's office has authority to enforce the new requirements and may bring a civil or criminal action to address violations. For example, the AG could seek other relief that may be appropriate to ensure compliance with the law or to recover direct economic damages resulting from the violation, or both. GDPR financial penalties can amount to 20 million euros, or 4 percent of a company's annual global revenue. California empowers its AG to impose major civil penalties for violations of its requirements: $2,500 per violation, which can be increased to $7,500 if the violation is intentional.

CI: *How has the Colorado law been received so far?*
KS: The new Colorado law is just part of the landscape. In my opinion, the GDPR and the California and Colorado laws will soon force a rewrite of our federal data privacy regulations. Although the U.S. does have some federal data privacy laws that govern specific business segments, such as the Health Insurance Portability and Accountability Act (HIPAA), it does not have a single law like the GDPR that covers all citizens. Unless a federal law is passed, each state's laws will have jurisdiction over its own citizens. I believe that the major players who market to U.S. consumers are lobbying Washington at this very minute to pass sweeping data privacy legislation that balances consumer rights with their ability to make a profit. Similar to how the Colorado law regarding marijuana is shaping the future of U.S. cannabis legislation, the Colorado data privacy law will help highlight the need for harmonized national data privacy legislation.

Chorus Consulting LLC

Colorado Data Privacy Law Compliance Checklist

90% of U.S. Companies Are Not Prepared

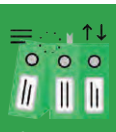
The EU's GDPR made the first big splash in May. The California Consumer Privacy Act passed in June and, when it goes into effect in 2020, will expand U.S. data privacy requirements. But Colorado was the first state to add its own new requirements, and the law went into effect in September.

What The New Colorado Law Requires:

- You must have a written policy explaining how you will dispose of the personal information and follow through on those procedures.
- If a data breach is detected, you must alert consumers that their data has been compromised within 30 days. If more than 500 Coloradans are impacted, the entity must alert the attorney general's office.
- You must take "reasonable" steps to protect the personal information you keep.

RECOMMENDED ACTIVITIES TO BECOME COMPLIANT

- ✓ Revise your document retention policy and department retention schedules to ensure the immediate destruction of paper and electronic documents containing personal information when that data is no longer necessary (e.g., applications for employment, school admissions, credit, insurance, or property rental; W2, I9, and building security employment documentation; patient medical or financial data; and computer user names and passwords).
- ✓ Map and inventory your organization's document and data storage end points (onsite, offsite, and cloud storage) to understand where documents and data with PII are being saved.
- ✓ Review, and if necessary, renegotiate, and revise contracts with any third-party vendors to require that they implement and maintain reasonable security procedures and practices that are (1) appropriate to the nature of the personal identifying information disclosed and (2) reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure or destruction.
- ✓ Put in place security procedures to protect, track, and report PII (e.g., encrypt documents and data with PII, implement a third-party utility to track the location and status of electronically stored PII throughout the infrastructure).
- ✓ Implement an incident response program to notify affected Colorado residents (and the Colorado Attorney General if more than 500 residents have been impacted) within 30 days after determining that a security breach occurred (this supersedes HIPPA's 60 day breach notification mandate).
- ✓ Perform employee training on this law and its mandate.


Information Governance


Data Security & Compliance


Digital Forensic Services


eDiscovery Services


Advisory Services

Contact Us: (832) 953-5743 | info@chorusconsulting.net | www.chorusconsulting.net