WARD AND SMITH, P.A.
ATTORNEYS AT LAW

In-House Counsel Seminar Insights: What Corporate Counsel Need to Know about Privacy and Data Security

Written By **Deana A. Labriola** (dl@wardandsmith.com)
January 11, 2019

Two Ward and Smith attorneys and the top information technology lawyer for a Fortune 250 company explained how companies seeking to keep their privacy and data security practices in line with the law face an increasingly complex legal environment.

Angela Doughty and Caroline Outten, Ward and Smith attorneys who hold the Certified Information Privacy Professional – United States credential, were joined by VF Corp.'s Matt Cordell for an in-depth panel discussion at Ward and Smith's 2018 In-House Counsel Seminar.

The experts explained that the legal landscape for data security and privacy issues is more complex than ever.

"We in the United States don't really have an overarching data privacy law," Outten said. "It's a patchwork of laws."

Not only are there federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), but there are a growing number of state laws and even local legislation. In addition, the European Union has implemented the General Data Protection Regulation (GDPR) — what Outten jokingly called the "Gosh Darn Privacy Regulation."

Every state now has a data breach law. Half a dozen states now have laws governing biometric data. And some municipalities, such as Chicago, are considering additional local laws. It's a lot with which to comply.

California Consumer Privacy Act

One major new law looming on the horizon is the California Consumer Privacy Act. The law is scheduled to go into effect in January of 2020, and its sweeping measures could affect a wide swath of organizations that have even modest connections to the Golden State.

"This is not a business-friendly proposal," Outten warned. Cordell predicted the law would be amended one more time before it goes into effect, but the measure will still probably mean major changes for businesses.

It would apply to any company collecting the personal information of California residents that also:

- Has more than $25 million in annual revenue companywide, or
- Buys, sells, receives, or shares information from 50,000 individuals, devices or households in California, or
- Derives more than half its revenue from selling personal information.

Affected organizations, Outten said, would be required to provide consumers significant information about a wide range of information an organization might collect — everything from information about a user's browser to biometric data, even "olfactory" information. Companies would also have to allow people to opt-out of information collection, among other provisions.

The California attorney general's office will handle enforcement, with civil penalties of up to $7,500 per incident for intentional violations and $2,500 per incident for unintentional violations. But consumers could also pursue violations of and recover $100 to $750 individually.

Litigation over data privacy grows

In addition to new laws on the books, the panelists warned of increasing litigation over health care data, website accessibility, privacy policies, the "internet of things," and concerns about minors.

"Something that's interesting is a recent trend towards tacking privacy claims onto accessibility claims," Cordell said. In those cases, a lawsuit about website accessibility will also have a claim related to privacy, arguing, in effect, that if a website isn't accessible, neither is its privacy policy, and therefore a company may be violating privacy laws.

Cordell noted that data security and privacy policies and practices are coming under scrutiny during business transactions too, such as mergers and acquisitions.

European regulators have started to enforce the GDPR, Cordell said, but enforcement targets seem to vary widely. UK regulators, for example, have gone after a Canadian company that collected information on UK voters. In Austria, a very small company faced an enforcement action because the business had a security camera facing into the street. Hospitals and mobile app developers have also been the target of enforcement in other nations. "It's really hard to glean from these any sort of trend or connecting line," Cordell said. A European colleague of his, he said, told him that "there's no rhyme or reason for who's getting hit with enforcement actions."

Five steps to operationalizing privacy and data security compliance programs

Doughty walked the seminar participants through a five-step process intended to help companies of all sizes and in all industry types with designing and operationalizing tailored privacy and data security compliance programs.

1. **Establish Governance.** The first step, Doughty said, is to establish how data will be managed and who is responsible for data security and privacy compliance in your company. Is it a centralized data management approach with a single individual or decentralized based on departments — perhaps a senior IT executive or a member of the in-house legal team — or the responsibility of a hybrid team comprised of a cross-section of people from a variety of departments? Regardless of governance type selected, it is vital for key stakeholders across the company — especially senior executives — to buy into and support the importance of this individual's or team's mission.

2. **Understand your current policies and practices.** Doughty said businesses collect tons of data every day. Many don't even know why they are collecting certain data, or many times, that it is even collecting the data at all. This makes assessing, tracking, and protecting data even more difficult. As a result, understanding current data collection practices can require multiple detailed conversations with people throughout your company — meetings they may feel they don't have time for — to understand what information your organization is collecting and why.

3. **Develop a privacy program framework.** With clear governance outlined and a sense of the data collection practices, you can now develop an overarching framework to support the governance team and implementation of the company's privacy and data security policies.

4. **Determine what laws and regulations apply to your business.** It's important to assess what local, state, national and international laws and regulations apply to your company's data collection practices, so you and others working on privacy compliance can determine your legal obligations and responsibilities. Doughty cautioned participants to be aware that privacy regulation applicability is based on the data collected, not the location of the company.

5. **Identify gaps in policies and develop a remedial action plan.** Finally, the privacy governance team should compare its current data and privacy practices with the identified legal obligations and responsibilities. Any gaps in current practice with the requirements of legal compliance should be identified and prioritized based on risk, and then a remedial action plan for compliance developed.

Even once this five-step process is completed, Doughty warned, the privacy and data security work isn't finished. Policies may need updates as new regulations take effect, new legal precedents are established, and company business practices change.

"It's good hygiene, every so often--at least once a year or when regulations are changing--to go back," she said. "Once you do this cycle a couple of times, it's not quite as difficult."

_____

This is one of a series of articles summarizing key takeaways from Ward and Smith's In-House Counsel Seminar. See additional articles:

- Managing Internal Corporate Investigations While Preserving Privilege
- How General Counsels can Successfully Collaborate with Outside Attorneys

--