

# INFORMATION SECURITY

---

## INFORMATION SECURITY AND PRIVACY LAW

### Protecting Your Business's Valuable Data

Information is the life's blood of any business, and almost all information generated today is in electronic form. Some of the information is company proprietary information and trade secrets. Other information is sensitive personally identifiable information, such as credit card and bank account information and protected health information in the healthcare field. Trust is presumed, and companies go to great lengths to ensure the security and protection of their sensitive information, including trade secrets and customer data.

Companies need robust protections for their trade secrets, financial data, medical records and other sensitive information. At Murphy Cooke Kobrick LLP, we bring hands-on experience and an ever-growing legal knowledge in high-level data protection.

Satisfaction of your customers is based on the security of their sensitive data. When security is breached, trust is violated with your customers taking their business elsewhere.

## HELPING TO PROTECT DATA AND HOLD PERSONNEL ACCOUNTABLE

We help companies when data is taken from them, whether by an insider or through the hacking of their systems. For instance, it is common for departing employees and independent contractors to take valuable trade secrets and confidential information. In such cases, we can assist in an internal investigation of the incident and follow-up actions.

Medical professionals face similar challenges. Doctors and hospitals must maintain high standards of confidentiality in ensuring the privacy and security of their medical records under health care privacy and security laws. When privacy is violated, we take action against the responsible party.

Also, information security lawsuits are becoming more common. If you had a breach, and someone sues your business for failing to take care of sensitive personal information, we can help defend your business in court. Likewise, we have been involved in cases in which former employees have been unfairly

accused of stealing data. We can help defend against such accusations in a lawsuit or facilitate an independent review of systems to show that no information was taken.

Finally, part of the confidence that we have earned from our business clients comes from helping them draft and implement security policies and procedures related to data protection, government regulatory compliance, and proper incident response practices. We help companies make breach notifications and follow up with security breaches to prevent future problems and liabilities.

Information security law is an emerging area of law focusing on one of our society's most valuable sources of wealth – information. Information security law is nothing new. Nonetheless, information security law is “emerging” in the sense that it has arisen largely in the last two decades, as opposed to more traditional areas of law, like real estate, that have been with us since the founding of the United States. It is also “emerging” because developments in the law have been accelerating in recent years.

Returning to the original question, then, what is information security law? Also, what do information security lawyers do?

Information security law, or infosec law, is in some ways a new area of law. In other ways, it is a new area of practice for law firms. And in yet other ways, it has an industry-specific focus. This article discusses all of these dimensions of information security law.

Information security, as an emerging area of law, includes a number of components. First and foremost, information security lawyers counsel their clients on requirements to keep data and information systems secure. These requirements may stem from public law (statutes and regulations) or private arrangements made via contracts. Infosec lawyers help clients answer the key question: What does my company really need to do to comply with infosec requirements under applicable law and contracts?

Second, infosec law addresses liability that arises from security breaches or defects in security products or services. Parties injured by a security breach may sue to seek damages or an injunction against the parties responsible for the breach. When the perpetrators are unable to be found or it isn't worth suing them, injured parties may sue others who allowed the breach to occur or failed to stop it. Companies purchasing security products or services may sue their vendors when the products or services don't work as advertised or when they fail to prevent a breach. Infosec lawyers bring suit on behalf of the injured party or defend these kinds of suits.

Third, infosec law covers secure electronic commerce. Secure electronic commerce answers questions such as:

- How do parties form contracts online?
- Are online contracts treated the same as paper contracts under the law?
- What must a person or business do to authenticate himself, herself, or itself to another party online?
- What must be done to tie an individual or business to an online transaction and hold that party accountable for it?
- What can show that a person has agreed to an online transaction: an electronic signature, a secure form of electronic signature, or a digital signature (a particular kind of secure electronic signature)? (I leave the discussion of the differences among these kinds of signatures for another day and article.)

Secure electronic commerce systems or programs may, for instance, establish a trading community in which a large organization can procure products or services from its vendors. Electronic “commerce” can also include e-government services. For example, an environmental regulatory agency may establish an online presence to accept submissions of environmental reports and disclosures. E-commerce lawyers counsel clients concerning ways to establish secure e-commerce systems, the interplay between background law and contracts involved in establishing these systems, and liability concerns arising from e-commerce activities.

Information security law, in addition to being an area of law, is also a law practice. Lawyers from a variety of traditional practice areas may work in the information security area. For instance, lawyers specializing in government regulatory matters may advise clients on federal or state statutes that impose infosec requirements. Attorneys working in government affairs in Washington or state capitols may become involved in lobbying efforts for or against new infosec legislation, such as the federal breach notification bills. Litigation lawyers are likely to be the professionals handling disputes arising from security breaches. Finally, members of technology transactions groups are often the first lawyers called in to counsel clients seeking to engage in secure e-commerce, although technology attorneys with the specialized skills needed to provide in-depth advice have created a distinct sub-specialty within the technology transactions umbrella.

Finally, information security lawyers focus on a particular industry: the information technology industry. Some law firms have IT law groups whose work includes addressing the specific needs of vendors of information security products and services. Infosec lawyers need to develop deep IT experience and exposure to clients that depend on IT for their operations and sometimes their entire livelihood. More recent trends, such as cloud computing, pose even greater challenges to the legal community.

Infosec lawyers cultivate contacts among IT professionals, and infosec professionals in particular. Servicing clients' infosec legal needs is a multi-disciplinary endeavor, and lawyers are creating fruitful partnerships and relationships with outside and in-house technical experts. Lawyers in the infosec field simply cannot perform their jobs alone. They require considerable assistance from experts with the technical expertise to provide comprehensive advice to clients.

In sum, information security is at once an emerging area of law, an area of practice, and an industry focus. As with new areas of the law in the past, attorneys practicing infosec law are those who have experience in allied areas of law, who have practices touching on a number of traditional practice areas, and who have IT and infosec technical expertise. The mix of technical and legal issues, the need to work with multi-disciplinary teams, and the novelty of the field challenge infosec lawyers, but make for a fascinating area of the law.