Data Protection 101

What Every DRI Member Should Know About Data Protection and Privacy

By Laura Clark Fey, April Falcon Doss, Brandon Hull, Stephen Reynolds, and Kirsten Small

Law firms are inviting targets for hackers. Given the nature of the legal industry, that fact is unlikely to change, but firms can take steps to keep themselves from being easy targets.

Introduction to the DRI Center for Law and Public Policy Electronic Privacy Working Group

Recognizing the growing impact of ever-evolving global data privacy laws on DRI's members, DRI's Center for Law and Public Policy created the Electronic Privacy Working Group (Working Group) this summer. Our Working Group falls under the auspices of the Legislation and Rules Committee, which is chaired by Gardner Duvall, partner at Whiteford Taylor and Preston LLP.

As a Working Group, we intend to use our deep privacy expertise to complement the work of DRI's Cybersecurity and Data Privacy Committee. Our goals include: (1) providing excellent, practical, educational materials concerning the electronic privacy and information security issues we anticipate are likely to be of highest interest to DRI members; and (2) helping DRI members stay on top of rapidly evolving global legislative and case law developments in the privacy field.

We have drafted this first article, "Data Protection 101," to provide DRI members with a high-level overview of key cybersecurity risks and key global data protection obligations imposed on corporations and law firms today. In this article, we provide basic information on the following topics:

- cybersecurity risks;
- lawyers' ethical duties in data protection;
- overview of challenges posed by data protection laws;
- key legal obligations and restrictions; and
- risks of non-compliance.

Cybersecurity Risks

When asked why he robbed banks, Willie Sutton is said to have quipped, "Because that's where the money is." If Slick Willie were a modern-day cybercriminal, he might be asked, "Why do you hack law firms?" The answer would be: "Because that's where the data is." Lawyers and law firms store vast amounts of confidential client information, both personal (health information, banking records, Social Security numbers) and corporate (trade secrets, draft SEC filings, merger negotiations). Cybercriminals often seek a particular type of information. Sometimes, it is a specific type of personal data, such as Social Security numbers. Other times, it is other data, such as confidential information concerning a corporation a law firm represents or its acquisition targets. In 2010, for example, a law firm in Toronto was handling the corporate takeover of a potash mining company. Seeking to disrupt the transaction, China-based cybercriminals worked their way down Bay Street, hacking one law firm after another until they found the law firm they were seeking.

The fact that the hackers in the Toronto case successfully infiltrated all seven law firms brings us to an uncomfortable truth: law firms are inviting and easy hacking targets. "Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing [inferior] safeguards… and (2) the information in their possession is more likely to be of interest to a hacker and likely to be less voluminous than that held by [their clients]." (ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 11, 2017).

Wholly apart from intentional targeting of law firms, many of the most common forms of cybersecurity incidents are initiated through automated software scanning that looks for vulnerabilities in networks and devices that are connected to the internet. These kinds of opportunistic cybercriminals are just as likely to find exploitable weaknesses in the IT networks of law firms, and in lawyers' personal accounts, as in the IT networks of their clients.

■ Laura Clark Fey, Privacy Law Specialist (IAPP), CIPP/US, CIPP/E, CIPM, FIP, leads Fey LLC, a privacy and information governance law firm in Leawood, Kansas, and has been selected by the European Commission and U.S. Department of Commerce as an EU-U.S. Privacy Shield Arbitrator. April Falcon Doss, partner and chair of cybersecurity and privacy at Saul Ewing Arnstein and Lehr LLP in Baltimore, Maryland, is a former associate general counsel for the U.S. National Security Agency. Brandon Hull, partner at Overturf McGaff and Hull PC in Denver, Colorado, is a diverse civil litigation and arbitration practitioner with a passion for privacy legislation. Stephen Reynolds, partner and co-chair of the data security and privacy practice at Ice Miller LLP in Indianapolis, Indiana, is a Certified Information Systems Security Professional (CISSP). Kirsten Small, CIPP/US, member of Nexsen Pruet LLC, is a litigator and appellate lawyer with an emphasis on privacy and information management. She practices out of the firm's Greensboro, South Carolina, office.





With annual statistics constantly showing the breadth and frequency of cyberattacks on the rise, all lawyers have good reason to be mindful of the privacy risks to information they maintain, as well as to the business interruption, costs, and reputational damage that can stem from attacks such as ransomware attacks.

Many lawyers and law firms are behind the curve when it comes to cybersecurity. The ABA 2018 Legal Technology Survey Report showed that many lawyers and law firms are not taking even basic security measures. For example, 72 percent of law firms reported they had not conducted a full security assessment; 75 percent had no incident response plan; 76 percent did not use full-drive encryption; 88 percent did not have remote data wiping capabilities; 71 percent did not use secure (encrypted) emails for confidential/privileged communications; 15 percent did not use any of the typical security measures available with respect to high-risk public wireless (WiFi) networks; and 60 percent had no disaster recovery or business continuity plan. And because only 34 percent of law firms have cybersecurity insurance, if a firm suffers a breach, the costs of remediating the breach, currently averaging around $4 million, will have to be borne by the firm.

The cybersecurity threats to law firms and corporations are myriad and ever-changing. It is easy for cybersecurity to drop a long way down on a priority list, especially when it involves understanding, implementing, and adapting new security protocols while simultaneously focusing on running a business and meeting client and customer needs. But the Willie Suttons of the world are still out there—they've just traded in their Tommy Guns for keyboards.

Lawyers' Ethical Duties in Data Protection

In April 2016, a massive breach of confidential client information at the law firm Mossack Fonseca made international news. Hackers had compromised the security of the firm's IT systems, and leaked information began appearing in headlines around the world. The data breach even got its own moniker: The Panama Papers. For lawyers and law firms, the Panama Papers case serves as a cautionary tale, reminding us that we have an ethical duty to protect the vast amounts of confidential information our clients entrust to us.

With annual statistics constantly showing the breadth and frequency of cyberattacks on the rise, lawyers have good reason to be mindful of the privacy risks to information they maintain, as well as to the business interruption costs and reputational damage that can stem from attacks like ransomware attacks. The rules of professional responsibility provide additional, important reasons for lawyers to focus on protecting the data in their possession from external cybersecurity incidents as well as from insider threats.

Several states have specifically promulgated ethics guidance—in the form of comments to professional rules, or ethics opinions—that makes clear that lawyers have a professional obligation to understand the technology they are using and how it could impact the confidentiality of information relating to client matters.

The ABA has issued guidance on how the Model Rules of Professional Conduct ("Model Rules") apply to data privacy and security, and a host of states have followed suit.

As a general matter, Model Rule 1.1 requires lawyers to demonstrate competence in handling client matters. In order "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology.*" By early 2019, nearly three dozen states had adopted this language imposing technology-related obligations under Rule 1.1.

In terms more specific to cybersecurity and data privacy, Model Rule 1.6 notes that lawyers have a duty to protect confidential client information and "*to take reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or access to, information relating to the representation of a client.*" Comment 18 is particularly relevant, noting that mere compromise of confidential client information is not a violation of the rules, "*if* the lawyer has taken reasonable efforts to prevent the unauthorized access or disclosure." In determining whether a lawyer's data handling practices are reasonable, the comment suggests that, "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use)."

Several states have specifically promulgated ethics guidance—in the form of comments to professional rules, or ethics opinions—that makes clear that lawyers have a professional obligation to understand the technology they are using and how it could impact the confidentiality of information relating to client matters.

In 2017, Florida became the first state to require technology-specific CLE for lawyers, requiring three technology-related credits in each reporting cycle. As the ABA and individual states continue to update ethics guidance relating to lawyers' use of technology, and as the landscape of cybersecurity risks increases while the framework of privacy protection laws becomes more complex, lawyers must pay more attention to understanding how they are using technology to manage clients' data, what risks are associated with those technologies, and how they, and others in their firm or their vendors, are safeguarding the information their clients entrusted to them.

Overview of Challenges Posed by Data Protection Laws

Compliance with state, federal, and international data protection laws is challeng-

ing, in part because of the sheer volume of such laws. There are currently hundreds of different global laws, and many more on the way.

In addition, compliance with data protection laws is challenging because of the breadth of actions covered by such laws. Many laws govern a broad range of personal data practices—from collection to final disposition of the data. Others govern specific practices, such as sending electronic marketing communications or monitoring employees.

Some laws are applicable to all types of personal data. Others impose obligations and restrictions on organizations concerning the collection, use, disclosure, retention, and security of specific categories of information, such as Social Security numbers and other national identifiers, driver's license information, children's data, financial or credit-related information, medical records, criminal justice records, and education records.

Some laws apply to all organizations collecting or receiving personal data. Others apply only to organizations in certain sectors. For example, there are laws applicable only to financial services organizations, such as the federal Gramm Leach Bliley Act, which requires financial services companies to secure non-public personal information (NPI) of customers; to restrict disclosure and use of NPI; and to notify customers when NPI is exposed to unauthorized persons.

Another reason data protection compliance is challenging is that laws in different jurisdictions governing the exact same practices (*e.g.*, notice, consent, third-party vendor contracting) can vary significantly.

Key Legal Obligations and Restrictions

As addressed above, data protection laws set forth widely varying data protection obligations and restrictions. Each organization must analyze the laws that apply to it and determine its own unique set of compliance obligations. Some of the most significant requirements are in the following areas:

- information security;
- notice/transparency;
- consent;
- third-party vendor contracting and management;
- data subject rights;
- employee monitoring;
- electronic marketing communications;
- data minimization;
- data destruction;
- data breach notification; and
- accountability practices/recordkeeping.

In this section of our article, we will provide a high-level overview of these data protection obligations and restrictions.

Information Security

Many countries, some federal agencies, and at least twenty-five states have laws that require organizations to protect the personal data they collect, store, and transfer. Most laws require only reasonable security procedures and practices that are appropriate to the nature of the personal data involved. However, some laws are very detailed in terms of the specific technical, physical, and administrative safeguards required for protecting personal data.

For example, Massachusetts requires organizations collecting personal data about Massachusetts residents to implement a comprehensive, written information security program (WISP) that meets very specific standards for safeguarding personal data in both electronic and paper format. Massachusetts recently raised the importance of compliance by amending its data breach notification law to require every organization experiencing a data breach to inform the Massachusetts Attorney General and the Massachusetts Director of Consumer Affairs and Business Regulation whether the organization maintains a WISP.

Another reason data protection compliance is challenging is that laws in different jurisdictions governing the exact same practices (*e.g.*, notice, consent, third-party vendor contracting) can vary significantly.

Notice/Transparency

Several data protection laws require organizations to provide notice to data subjects about their data collection, usage, and protection practices. Laws vary in terms of what must be covered in a privacy notice or statement, but many require notification of the categories of personal data collected; the purposes for which personal data is used; the types of third parties with which personal data will be shared; the reasons for sharing such personal data; and any applicable data subject rights.

Consent

Some data protection laws require that consent be obtained from a data subject before personal data is collected and/or used for certain purposes or for new purposes. Certain laws, such as the EU's General Data Protection Regulation, set forth the specific type of consent that is required (*e.g.*, freely given, specific, informed, unambiguous consent given by a statement or clear affirmative action). Many laws permit an opt-out approach in which consent is assumed if a data subject does not object or "uncheck" a checked box.

Third-Party Vendor Contracting and Management

Some data protection laws impose specific requirements on organizations to enter into written agreements with their third-party vendors that include specified provisions relating to privacy and security. The requisite terms vary, depending on the law at issue. Some data protection laws also mandate vendor oversight.

Data Subject Rights

A number of data protection laws provide for specific data subject rights. Rights given to data subjects include the right to access their personal data; to correct incorrect or outdated personal data; to delete their personal data; to transfer their personal data; to object to or opt-out of certain uses or sharing of their personal data; to withdraw consent to the processing of their personal data; and not to be discriminated against for exercising their data subject rights. Data subject rights laws vary significantly in terms of the specific rights provided, the circumstances under which data subject rights may be exercised, and deadlines for addressing data subjects' requests.

Employee Monitoring

Laws in certain states and countries regulate employee monitoring—most typically with respect to notice and consent. For example, states such as Connecticut and Delaware expressly prohibit employers from electronically monitoring employees without giving prior notice.

Electronic Marketing Communications

There are extensive international laws setting forth obligations and restrictions on electronic marketing practices. Obligations can vary significantly by state and country. Obligations also vary depending on the type of communication at issue (*e.g.,* text, email, facsimile, or telephone communication). Electronic marketing communications laws often prohibit deceptive practices. Key obligations that may be imposed include identifying the communication as a solicitation or advertisement; obtaining consent from recipients; providing recipients with an opt-out opportunity; and registration and licensing obligations.

Data Minimization

Many data protection laws require that organizations apply the principle of data minimization to limit the personal data that may be collected and to limit the time period for which such personal data may be used and stored. With respect to the latter point, the data minimization principle generally prohibits organizations from keeping personal data for a longer period than is necessary to fulfill the original basis for collecting and processing the data.

Data Destruction

Many data protection laws require organizations to ensure personal data is unreadable or indecipherable at the time organizations dispose of such data. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (Security Rule) requires implementation of reasonable policies and procedures to address the disposal of electronic Protected Health Information (PHI) and the hardware or electronic media on which it is stored, as well as procedures for removing electronic PHI from electronic media before the media are made available for re-use. The Security Rule also requires training workforce members on disposal policies and procedures.

Data Breach Notification

There are a multitude of data breach notification laws at the state, federal, and international level. For example, all fifty states, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, have their own unique data breach notification laws in place. Data breach notification laws vary significantly, including with respect to what constitutes a breach; who must be notified; time limits for providing notification; what must be included in the breach notification; and whether and under what circumstances credit monitoring or identity theft protection service must be provided.

Accountability Practices/Recordkeeping

Some data protection laws require organizations to maintain documentation of their compliance with data protection obligations. Some of the records that must be retained are quite detailed. *See, e.g.*, Article 30 of the GDPR (enumerating specific information to be covered in records of data processing activities).

Risks of Non-Compliance

Non-compliance with data protection laws can result in significant risks for a business. These risks extend well beyond legal liability.

Risks arising from regulatory actions include steep financial penalties (up to 4 percent of annual worldwide revenues or €20 million, whichever is higher, in the case of the GDPR). The amounts imposed by regulators are growing. This summer, the U.K.'s data protection authority announced its plan to fine British Airways £183 million. In the U.S., regulators announced their settlement with Equifax in which Equifax agreed to pay between $300 million and $425 million to the people whose data was exposed, and another $275 million in civil penalties to forty-eight states, Washington, D.C., Puerto Rico, and the Consumer Finance Protection Bureau. Regulators are getting more comfortable handing down fines totaling hundreds of millions, and even billions, of dollars.

Although financial penalties seem to get the most "play" in the news, some of the other sanctions that regulators are authorized to impose could actually cause more harm to organizations than the fines. For example, laws may permit regulators to issue a temporary or permanent ban on data processing (including data collection, storage, and handling); to order the erasure of data; to implement new security protocols; or to suspend cross-border transfers of data. Additionally, some laws permit the imposition of criminal penalties, including prison sentences and personal fines.

In addition to the risk of being hit with regulatory sanctions, organizations risk being confronted with class actions and individual litigation, which can, of course, also take a toll financially. And some laws provide for joint and several liability, so that even if an organization's vendor was the primary cause of a breach, the organization that hired the vendor could be held fully liable for the breach.

Finally, there is the risk of harm to an organization's reputation, value, and overall health. For example, as a result of the data breach suffered by Equifax, the company had its credit outlook downgraded by Moody's from "stable" to "negative." This was the first time in history that a company had its credit outlook downgraded as a result of a cyberattack. When it comes to the valuation of an organization, a 2018 analysis indicated that companies that suffer a data breach see their share prices fall an average of nearly 3 percent after a data breach is announced. https://www.comparitech.com/blog. In instances where more sensitive personal information (*e.g.*, credit card information, Social Security numbers, etc.) is compromised, share prices generally drop even more. Although prices may rebound in the weeks after the breach, in the long term, breached companies have been shown to underperform the market.

Conclusion

In conclusion, we hope our Data Protection 101 article provides you with a helpful overview of key legal and ethical obligations imposed on corporations and law firms, as well as the key risks of non-compliance. Please reach out to the working group chair, Laura Clark Fey, at lfey@feyllc.com, if you have specific topics you would like our Working Group to address, or if there are specific resources you would like our Working Group to provide. FD