

HUNTON & WILLIAMS

Law Firms Face Risks in Handling Personal Information

By: **Lisa J. Sotto, Aaron P. Simpson, and Boris Segalis**

This article seeks to provide an overview of key privacy and information security issues impacting the practice of law. Law firms may collect, use and disclose personal information in numerous circumstances, both as providers of legal services and as employers. In safeguarding personal information that pertains to their employees or clients, or other individuals, law firms must comply with applicable privacy and information security laws as well as their professional duty of confidentiality. The article provides an overview of potential legal issues that law firms may encounter in connection with (i) hiring and employee administration functions; (ii) safeguarding the security of personal information that a law firm maintains; (iii) managing service providers that access personal information for which the firm is responsible; (iv) handling information security breaches; and (v) operating the firm's Internet assets. The article also touches on privacy and information security laws outside the United States, including the legal requirements relevant to cross-border transfers of personal information. The final topics the article addresses are examples of privacy and information security enforcement actions, including judicial enforcement of professional ethics rules, and a brief discussion of some of the key pending privacy and information security legislative initiatives.



Lisa J. Sotto
(212) 309-1223
lsotto@hunton.com



Aaron P. Simpson
(212) 309-1126
asimpson@hunton.com



Boris Segalis
(212) 309-1289
bsegalis@hunton.com

Lisa J. Sotto is a partner and head of the privacy and information management practice at Hunton & Williams. Aaron P. Simpson is a partner in the practice, and Boris Segalis is a senior associate at the firm.

Table of Contents

Introduction..... 1

Privacy and Information Security Laws..... 1

What is Personal Information? 3

Law Firms’ Role in Handling Personal Information 5

U.S. Privacy and Information Security Issues Affecting Law Firms..... 6

Employee Privacy..... 6

Background Checks..... 6

Employee Monitoring 7

Information Security 9

Information Security Program Requirements 9

Social Security Number Laws..... 10

Security of Health Information..... 11

Vendor Management 12

Disposal of Records..... 12

Information Security Breaches..... 13

Online Privacy 14

Privacy and Information Security Requirements Outside the U.S..... 15

Cross-Border Transfers of Personal Information 16

Enforcement Actions for Privacy and Information Security Violations 18

Professional Ethics Considerations 19

Future Trends in Privacy Regulation 20

Conclusion 22

Introduction

The modern global economy demands robust information about individual consumers and employees that is accurate, current and increasingly specific. While businesses have expanded their collection and use of such information to meet demand, this expansion simultaneously has raised weighty concerns about privacy and information security, including for law firms. Given the significant risks associated with the collection and use of personal information, it is imperative that law firms understand the key privacy and information security issues impacting the practice of law. This article seeks to provide an overview of these issues.

Privacy and Information Security Laws

Countries throughout the world have been increasingly active in enacting privacy and information security laws over the past two decades. Privacy laws generally govern the processing of personal information, including its collection, use and disclosure. Information security laws focus on the protection of personal information against compromise, such as accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use. In the U.S., there are numerous privacy and information security requirements that could impact law firms, at both the federal and state levels, including:

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM”),¹ which governs email marketing;
- the Electronic Communications Privacy Act (“ECPA”), including the Wiretap Act² and Stored Communications Act (“SCA”),³ which governs the interception and review of electronic and wire communications;
- the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”),⁴ whose regulations govern privacy and data security issues related to health information (including data maintained by employee health plans);

¹ 15 U.S.C. §§ 7701–7713.

² 18 U.S.C. §§ 2510-22.

³ 18 U.S.C. §§ 2701-12.

⁴ 42 U.S.C. §§ 1320d–1320d-8.

- the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”),⁵ which imposes additional information security obligations on HIPAA covered entities and business associates of covered entities;
- the Fair Credit Reporting Act (“FCRA”)⁶ and the Fair and Accurate Credit Transactions Act (“FACTA”),⁷ which address information security and identity theft, and govern the use and disclosure of consumer reports;
- state laws requiring the provision of privacy notices to individuals, such as the California Online Privacy Protection Act;⁸
- state information security breach notification laws, which are in place in over 45 states, Washington, D.C. and Puerto Rico;⁹
- state laws imposing minimum information security requirements, such as the Massachusetts Standards for the Protection of Personal Information;¹⁰
- state laws that regulate the collection, use and other processing of Social Security numbers (“SSNs”);¹¹ and
- state laws requiring the secure disposal of records containing certain personal information.¹²

In addition to these laws and requirements, the Federal Trade Commission (“FTC”) employs its authority under Section 5 of the Federal Trade Commission Act (the “FTC Act”)¹³ to take enforcement actions against entities whose privacy or information security representations or practices the FTC deems unfair or deceptive. The FTC’s Section 5 authority is discussed in more detail below.

Notably, courts have exempted law firms from some U.S. privacy and information security laws. Specifically, courts have ruled that law firms are not “financial institutions” within the meaning of the Gramm-Leach-Bliley Act (“GLBA”), exempting law firms from the

⁵ American Recovery and Reinvestment Act of 2009 (ARRA), §§ 13,001–13,424, 4001–4302, Pub. L. No. 111-5, 123 Stat. 260.

⁶ 15 U.S.C. § 1681(a)–(b).

⁷ 15 U.S.C. §§ 1681–1681x.

⁸ Cal. Bus. & Prof. Code §§ 22,575–22,579.

⁹ *See, e.g.*, Cal. Civ. Code §§ 1798.29, 1798.82; N.Y. Gen. Bus. Law § 899-AA.

¹⁰ *See, e.g.*, 201 Mass. Regs. Code §§ 17.01–17.05.

¹¹ *See, e.g.*, Cal. Civ. Code § 1798.85.

¹² *See, e.g.*, Cal. Civ. Code § 1798.85.

¹³ 15 U.S.C. § 45.

Act's and the implementing regulations' information security requirements and certain privacy requirements.¹⁴ More recently, a federal court found that law firms are not subject to the FTC's Identity Theft Red Flags Rule.¹⁵ The Red Flags Rule implements certain provisions of the FCRA and, in relevant part, requires certain entities to develop and implement a written identity theft prevention program. But for these exceptions, most privacy and information security laws apply in the law firm context, and firms should understand the scope of their obligations.

What is Personal Information?

The starting point for discussing privacy and information security issues is understanding what information is deemed "personal" and, consequently, protected by relevant legal requirements. Although the contours of the legal definitions of personal information vary depending on the particular laws and the specific activities being regulated, the overarching concept is that personal information is any information that relates to, or can be used to identify, an individual.

Unlike the European Union, which takes a comprehensive view of privacy law and thus has a uniform definition of "personal data," the U.S. takes a sectoral approach to regulating privacy and information security. As a result, state and federal laws define "personal information" differently. For example, most state information security breach notification laws define personal information narrowly to include a first name or first initial and last name in combination with (i) an SSN, (ii) a driver's license number or state ID card number, or (iii) a combination of an account number or credit or debit card number with any security code, access code or password, such that the combination would permit access to an individual's financial account.¹⁶ Federal laws and regulations, such as HIPAA, GLBA and the FTC's Financial Privacy Rule, on the other hand, take a broader view and deem any information about an individual that identifies the individual to be personal information.¹⁷

For law firms, the definition of personal information the FTC has applied in its privacy and information security enforcement actions under Section 5 of the FTC Act is the most relevant. The FTC defines personal information as individually identifiable information that is

¹⁴ See *ABA v. FTC*, 430 F.3d 457 (D.C. Cir. 2005).

¹⁵ See *ABA v. FTC*, 671 F. Supp. 2d 64 (D.D.C. 2009).

¹⁶ See, e.g., Ariz. Rev. Stat. § 44-7501.

¹⁷ See, e.g., HIPAA Privacy Rule, 45 C.F.R. § 160.103; GLBA, 15 U.S.C. 6809(4); FTC Financial Privacy Rule,

¹⁶ C.F.R. § 313.3(n).

from or about an individual including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name, that reveals an individual's email address; (d) a telephone number; (e) an SSN; (f) credit or debit card information, including card number, expiration date or data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number or check number; (h) a driver's license, military or state identification number; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; or (j) any information that is combined with any of (a) through (i) above.¹⁸

It is important to understand that the definition of personal information is a moving target. The regulators' views of what information may be deemed personal by no means remain static. Technological advancements that allow various data elements from many sources to be easily combined make it difficult if not impossible to establish a finite set of data elements that can identify an individual and, therefore, warrant legal protection. The FTC has acknowledged this challenge in the agency's self-regulatory principles for online behavioral advertising.¹⁹ The FTC noted that the traditional notion of what constitutes personally identifiable information versus non-personally identifiable information is becoming less and less meaningful and, therefore, should not by itself determine how the information should be protected.²⁰

¹⁸ See, e.g., Agreement Containing Consent Order at 2, *In re Dave & Buster's Inc.*, No. 0823153 (F.T.C. March 25, 2010).

¹⁹ FTC, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 12, 2009) at 20-25, available at <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

²⁰ See *Id.*

Law Firms' Role in Handling Personal Information

Law firms may encounter privacy and information management issues in numerous circumstances. As employers, for example, law firms may collect and process candidates' and employees' payroll, retirement plan and health benefits information. Firms may, for example, monitor communications employees send or receive via a firm's computer systems. Law firms also handle personal information of vendors, visitors and other individuals. Further, in their role as providers of legal services, law firms may receive records containing personal information from clients, clients' adversaries and other parties. Personal information (including financial account information, medical information and personal communications) may be contained in records a law firm receives and reviews in connection with litigation discovery, due diligence for a corporate transaction or an internal investigation a firm undertakes on behalf of a client. When providing services to individuals, such as advising on trusts and estate matters or family law matters, law firms may handle highly confidential personal information. Law firms also routinely provide access to personal information to third parties, such as technology vendors that assist in processing clients' documents or entities that provide services to the firm's employees.

Regardless of the circumstances in which a law firm handles personal information, the firm must appropriately safeguard the information to protect the interests of the firm and its clients. Law firms are uniquely positioned in that their need for adequate privacy and information security procedures arises not only from the obligations imposed by privacy and information security laws. Lawyers are bound by a professional duty of confidentiality, which is a paramount component of the attorney-client relationship.²¹ A law firm's failure to safeguard personal information that results in an unauthorized disclosure may result in not only a legal enforcement action against the firm, but financial and reputational harm to the firm's clients and, potentially, irreparable harm to one of the firm's most valuable assets – its reputation.

²¹ See, e.g., Confidentiality of Information, Model Rules of Prof'l Conduct R. 1.6.

U.S. Privacy and Information Security Issues Affecting Law Firms

Privacy and information security considerations may affect many aspects of a law firm's operations. Below are examples of some of the key privacy and information security issues that law firms should consider in understanding their obligations in connection with collecting, using, disclosing or otherwise processing personal information.

Employee Privacy

Privacy and information security laws in the U.S. impose a variety of requirements with respect to handling employees' personal information, including the collection, use, disclosure, safeguarding and disposal of the information. Here are some of the aspects of the employment relationship that these privacy requirements may impact.

Background Checks

When considering job applications, employers have the ability to discover through various public and non-public sources a significant amount of information about applicants. Employers may, for example, obtain information from consumer reporting agencies, investigators, Internet search engines or social networking websites.

Employers often ask consumer reporting agencies to provide information about job applicants or employees, including professional and personal details, educational credentials, and criminal background. In doing so, employers must comply with legal obligations. Pursuant to the FCRA, for example, an employer must disclose to a job applicant or employee that the employer will request a consumer report about the individual from a consumer reporting agency, and obtain the individual's signed consent prior to requesting the report.²² If the employer intends to use the information contained in the consumer report in connection with an "adverse action" (*e.g.*, a decision not to hire or promote, a rescission of an existing job offer, or a reassignment or demotion), the employer must provide notice of the adverse action to the individual, including notice of the individual's right to obtain a copy of the consumer report.²³ An employer requesting a consumer report also may be required to certify to the consumer reporting agency that it has complied with relevant FCRA requirements. Many states have enacted laws that are similar to the FCRA and contain provisions requiring notice to and consent

²² 15 U.S.C. § 1681b(b).

²³ 15 U.S.C. § 1681a(d)(1).

of job applicants or employees before requesting a background check for employment purposes from a consumer reporting agency.²⁴

Employers also increasingly seek information about prospective and current employees from online sources, including social networking sites, that may contain information such as an individual's age, race, marital status, sexual orientation, political affiliation and opinions. While there may not be a legal requirement currently in effect in the U.S. that prevents employers from gathering publicly available information on the Internet, taking adverse action on the basis of this information may create reputational risk. For example, if a law firm withdraws an employment offer on the basis of unsubstantiated information obtained through an Internet search, the firm's actions may become public (by, for example, being posted on a well-read legal blog). The publicity may embarrass the firm, make it difficult for the firm to recruit law school graduates, and create an impression among clients that the firm is careless and insensitive to confidentially issues. If publicly-available information a firm collects on the Internet includes details about protected characteristics, such as a disability, family status or sexual orientation, an adverse action may create a risk of litigation. Finally, firms should verify that their use of third party websites is consistent with the sites' terms of use. Using a site in violation of its terms creates legal and reputational risks.

Employee Monitoring

The monitoring of employee communications raises privacy concerns, and is currently the subject of significant and high profile litigation. Changes in electronic communication technologies, monitoring technologies and the increasing use of monitoring in the business context, in combination with employees' reliance on the Internet, email and instant messaging in conducting their daily lives, have challenged existing notions of employee privacy. The extent of employee privacy expectations in the workplace was one of the issues considered by the U.S. Supreme Court in *City of Ontario v. Quon*²⁵ and was the subject of a recent New Jersey Supreme Court decision in *Stengart v. Loving Care Agency, Inc.*²⁶

²⁴ See, e.g., Vt. Stat. Ann. tit. 9, § 2480a *et seq.*

²⁵ In *City of Ontario v. Quon*, the U.S. Supreme Court discussed a public employee's expectation of privacy in text messages sent over an employer-issued device. The Court did not rule on these privacy issues, however, instead finding that the search of the messages was reasonable under the circumstances irrespective of the employee's expectations of privacy. 2010 U.S. LEXIS 4972 (June 17, 2010).

²⁶ 990 A.2d 650 (addressing an employee's expectation of privacy in workplace email communications).

Law firms have a legitimate interest in monitoring their employees' communications to safeguard against inappropriate use of a firm's resources. Misuse of the firm's resources diminishes productivity, risks exposure of confidential firm or client information, and may expose computer networks to overload, viruses and hackers. There are limits, however, on the monitoring of employees in the workplace. In the U.S., the ECPA and various state laws impose certain restrictions on the monitoring and review of employees' communications. Specifically, in certain circumstances, these laws may prohibit the interception of communications (such as emails, instant messages or text messages, and telephone calls) without the consent of one or both parties to the communication. In addition, the laws may require employee consent to the review of electronic communications held in storage. Law firms must carefully consider these legal requirements in implementing their communications monitoring programs.

Many federal and state court decisions that address an employee's expectation of privacy in the workplace suggest that key elements in complying with relevant federal and state privacy requirements include (i) developing a comprehensive communications policy that governs the use of an employer's electronic communications resources, and (ii) providing employees with a clear notice of the employers' communications monitoring practices.²⁷ Some states, such as Connecticut and Delaware, require by statute that employers notify employees of their workplace communications monitoring practices.²⁸

A law firm's communications policy should contain an unambiguous statement that the firm's communications systems are intended for business use and that all communications, regardless of their content, are subject to monitoring. The policy should provide a description of the monitoring methods the firm might use and indicate that employees should have no expectation of privacy in their communications when using the firm's systems. If the firm intends to monitor communications employees may send via their workplace computers using private web-based accounts, the policy should be explicit in this regard. The policy should explicitly indicate the consequences of non-compliance. Employees should be required to acknowledge in writing the policy before being allowed to access the firm's systems. To the extent a law firm uses a third party to provide communications services to its employees, the

²⁷ See, e.g., *Long v. Marubeni Am. Corp.*, 05 Civ. 639 (GEL)(KNF), 2006 U.S. Dist. LEXIS 76594, at *7-9 (S.D.N.Y. Oct. 19, 2006) (statement in an employer's policy that employees "have no right of personal privacy in any matter stored in, created, or sent over the e-mail, voice mail, word processing, and/or Internet systems provided" by the employer quashed employees' expectation of privacy when using company computers or systems); see also *Stengart*, 990 A.2d 650.

²⁸ See, e.g., Conn. Gen. Stat. § 31-48d; Del. Code Ann. tit. 19, § 705.

firm should require employees to consent to the service provider's disclosure of the communications to the firm. Finally, the firm's actual monitoring practices should be consistent with its policies.

Information Security

In the U.S., information security laws have been enacted at both the federal and state levels. As a result, organizations in the U.S. often may be subject to numerous overlapping requirements. The federal laws are generally sector-specific, while state laws impose information security requirements on organizations that either do business in the particular state or process personal information about the state's residents. Numerous states also have passed laws specifically regulating organizations' use of Social Security numbers. Notably, some of the state information security laws effectively create national standards both because of the size of their populations and economies and because organizations operating nationwide may implement state requirements across the organization to streamline their information security practices. In addition to federal and state requirements, some industry groups, such as the Payment Card Industry Security Standards Council, have adopted self-regulatory information security frameworks. Below are several examples of federal and state information security requirements of which law firms should be aware when handling personal information.

Information Security Program Requirements

A number of states require organizations to develop and implement information security programs designed to safeguard personal information. For example, California law requires businesses that own or license certain personal information about California residents to (i) implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification or disclosure, and (ii) contractually require nonaffiliated third parties to which they disclose personal information to maintain reasonable security procedures.²⁹ Arkansas, Connecticut, Maryland, Nevada, Oregon, Rhode Island, Texas and Utah have enacted similar laws.³⁰ The California law does not define what information security practices are "reasonable," leaving law firms to determine the types of security measures that are reasonable and appropriate in light of the scope of their operations and

²⁹ Cal. Civ. Code § 1798.81.5.

³⁰ See, e.g., Ark. Code Ann. §§ 4-110-101 to 4-110-108; Conn. Gen. Stat. Ann. § 42-471; Md. Code Ann., Com. Law §§ 14-3501 to 14-3503; Nev. Rev. Stat. § 603A.210; Or. Rev. Stat. § 646A.622; R.I. Gen. Laws § 11-49.2-2; Tex. Bus. & Com. Code Ann. §§ 72.001–72.051; Utah Code Ann. §§ 13-44-101 to 13-44-301.

the nature and sensitivity of the personal information they process. In addition, law firms subject to the law must monitor third parties with whom they share personal information (such as service providers) and require the third parties by contract to implement appropriate security measures. Given the geographic reach of many businesses, this California law effectively imposes a national standard on businesses that maintain personal information. This law may apply, for example, to a law firm located in New York that obtains records containing information about California residents from a client located in California.

Unlike state statutes that require organizations to maintain reasonable security of personal information, Massachusetts has promulgated regulations that impose specific, strict information security requirements.³¹ The Massachusetts regulations came into effect on March 1, 2010 and apply to entities that own or license personal information about Massachusetts residents. The regulations require organizations to develop, implement and maintain a written, risk-based information security program that takes into account the organization's size, the nature of its business, the types of records it maintains and the risk of identity theft posed by the organization's operations. Also set forth in the regulations are specific administrative, technical and physical safeguards that the information security program must include. With respect to service providers, organizations are required to (i) take steps to select and retain service providers that are capable of appropriately safeguarding personal information, and (ii) have in place a contract with each relevant service provider that governs the protection of personal information. Given the nature of legal practice, law firms may be in the position of a service provider pursuant to these regulations. Thus, law firms can expect firm clients to contractually mandate that the firm implement personal information safeguards that comply with the regulations to the extent they have access to personal information.

Social Security Number Laws

Social Security numbers are commonly used by employers to identify employees and keep track of employment-related records. Law firms may handle SSNs of their employees as well as those contained in client or third party records. To combat identity theft, more than thirty states have adopted legislation imposing restrictions on the processing of SSNs.³² While these

³¹ 201 Mass. Regs. Code §§ 17.01–17.05.

³² See, e.g., Ariz. Rev. Stat. § 44-1373; Colo. Rev. Stat. § 6-1-715; Haw. Rev. Stat. Ann. §§ 487J-2 to 487J-3; 815 Ill. Comp. Stat. Ann. 505/2RR, 505/2QQ; Md. Code Ann., Com. Law §§ 14-3401 to 14-3403; Mich. Comp. Laws Serv. §§ 445.81–445.87; Minn. Stat. Ann. § 325E.59; N.J. Stat. Ann. § 56:8-164; N.Y. Gen. Bus. Law § 399-dd;

SSN restrictions differ, many states have implemented the California model adopted in 2001 and set forth in the California Civil Code.³³ The California law prohibits (i) publicly posting or displaying an SSNs, (ii) printing an SSN on any card required to access products or services, (iii) requiring an individual to transmit his or her SSN over the Internet unless the connection is secure or encrypted, (iv) requiring an individual to use his or her SSN to access an Internet website, unless a password or other unique personal identification number or authentication device is also required to access the site, (v) printing an individual's SSN on any materials that are mailed to the individual, or (vi) encoding or embedding an SSN in or on a card or document, including but not limited to using a bar code, chip, magnetic strip or other technology in place of removing the SSN. Notably, Connecticut, Michigan and Texas require organizations to create and publish policies regarding their collection and use of SSNs.³⁴ Finally, recent amendments to the Federal Rules of Civil Procedure restrict certain uses of SSNs in public court filings.³⁵

Security of Health Information

The privacy and security of health information has long been governed by HIPAA, which applies to entities in the health industry, such as doctors, hospitals and health management organizations.³⁶ The recent enactment of the HITECH Act, however, has expanded the scope of entities subject to HIPAA's information security requirements.³⁷ For example, pursuant to the HITECH Act and the U.S. Department of Health and Human Services regulations that implement the Act, law firms that provide services to HIPAA covered entities and receive certain personal health information from the entities or their service providers in connection with the representation likely will be required to fully implement the information security safeguards specified by the HIPAA Security Rule. The Security Rule mandates a written, comprehensive information security program that includes specific administrative, physical and technical information security safeguards set forth in the Rule.³⁸

N.C. Gen. Stat. § 75-62; Okla Stat. Ann. tit. 40, § 173.1; Pa. Stat. Ann. § 201; R.I. Gen. Laws § 6-48-8; S.C. Code Ann. § 37-20-180; Tex. Bus. & Com. Code Ann. § 501.002; Vt. Stat. Ann. tit. 9, § 2440.

³³ Cal. Civ. Code §§ 1798.85–1798.89.

³⁴ See Conn. Gen. Stat. Ann. § 42-471; Mich. Comp. Laws Ann. § 445.84; Tex. Bus. & Com. Code Ann. § 501.052.

³⁵ See Fed. R. Civ. P. 5.2.

³⁶ 42 U.S.C. §§ 1320d–1320d-8.

³⁷ ARRA, 123 Stat. 260.

³⁸ See 45 C.F.R. §§ 164.308, 164.310, 164.312.

Vendor Management

Law firms typically retain a variety of third party service providers. These service providers may have access to personal information when they process the firm's payroll, provide benefits to the firm's employees, provide technical support to the firm's personnel, or manage client or third party records. Allowing service providers to access personal information raises several privacy and information security issues. For example, if a service provider suffers an information security breach that involves personal information processed on behalf of the firm, the firm likely will have obligations to notify affected individuals and third parties of the breach. In addition, as discussed above, various service provider oversight requirements exist under federal and state laws and other privacy regimes.³⁹ Regardless of the legal requirements, it is advisable for law firms to require their service providers to sign a privacy, confidentiality and information security agreement that limits how service providers may use or disclose the personal information they process on behalf of the firm and requires the service providers to implement appropriate security measures to safeguard the information.

Disposal of Records

In light of growing concerns about identity theft and heightened awareness of privacy issues, state and federal rules have been promulgated to help ensure that organizations securely dispose of consumer reports or other records containing personal information. For example, to the extent a law firm maintains consumer reports about employees, clients or other individuals, the firm must comply with the various state and federal requirements regarding the disposal of such information. Relevant regulations may include the FTC Disposal Rule, which requires secure disposal of any record about an individual that is a consumer report or is derived from a consumer report.⁴⁰ In addition, several states, including California, Georgia, Indiana, Montana, New Jersey, New York, North Carolina, Texas, Utah, Vermont, Washington and Wisconsin, have enacted laws that govern the disposal of certain personal information.⁴¹ While in some states the laws apply only to personal information that a customer provides to a business in exchange for a product or service, other states regulate the disposal of personal information regarding any individual, whether a client or an employee.

³⁹ See, e.g., ARRA, 123 Stat. 260; 201 Mass. Regs. Code § 17.03.

⁴⁰ See 16 C.F.R. pt. 682.

⁴¹ See e.g., Cal. Civ. Code § 1798.81; Ga. Code Ann. § 10-15-2; Tex. Bus. & Com. Code Ann. §§ 72.001–72.051; Wash. Rev. Code Ann. § 19.215.020(1).

Information Security Breaches

Law enforcement authorities in the U.S. have warned that law firms maintain a tremendous concentration of very critical, private information.⁴² As a result, infiltrating a law firm's computer systems is one of the optimal ways to obtain economic information that also may include personal information. Indeed, computer systems of U.S. law firms have reportedly been repeatedly targeted by hackers.⁴³

In one incident, for example, a law firm that filed a lawsuit against the Chinese government was subjected to a cyber attack by trojan-laced emails.⁴⁴ The hackers used "spear phishing" attacks – personalized emails drafted to look like they come from a trusted or reputable source and designed to induce the reader to click an attachment or link that will infect his or her computer with malicious software. In this case, the emails attempted to trick recipients into clicking on a link or attachment, which, in turn, contained malware. Although, in this incident, the messages appeared to recipients to come from other members of the firm, the phrasing of the messages tipped recipients off to the nefarious nature of the communications. The firm did not have a formal information security program, but employees had been warned not to open documents or click on links if they seemed suspicious. Another attack on a major New York law firm also has been linked to a group in China.⁴⁵ In this case, the hackers appeared to target the firm because it was negotiating a major international deal, seeking to steal documents pertaining to the firm's clients. These and other intrusions into computer systems of law firms or their service providers may result in legally cognizable information security breaches requiring significant remediation.

As discussed above, the vast majority of states have enacted laws to require notification of individuals affected by an information security breach. The effect of each state having enacted a distinct breach law is that an organization that experiences an information security breach must comply with the legal requirements regarding breach notification in each state in which affected individuals reside. As a result, an organization that suffers a breach must

⁴² James Rogers, *A Breach Too Far: Cybersecurity Concerns May Foster Changes in Lawyer Ethics Rules*, ABA J. (Feb. 1, 2010), at http://www.abajournal.com/magazine/article/a_breach_too_far/.

⁴³ Thomas Claburn, *Law Firm Suing China Hit By Cyber Attack: Targeted E-mail Messages Tried to Trick Recipients Into Clicking On Malicious Links*, Information Week (Jan. 14, 2010), at <http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=222301001>.

⁴⁴ *See Id.*

⁴⁵ Lolita C. Baldor, *FBI alert says hackers increasingly targeting Lawyers Offices, Public Relations Firms*, the Washington Examiner (Nov. 17, 2009), at <http://www.washingtonexaminer.com/economy/ap/70270057.html#ixzz0oFoEgCnN>.

understand and respond to the various notification requirements of each of the relevant jurisdictions. The laws generally require notification of affected individuals if (i) unencrypted personal information is reasonably believed to have been accessed or acquired by an unauthorized person, and (ii) the unauthorized access or acquisition is reasonably likely to compromise the confidentiality of the information. Over half of state breach laws employ a uniform definition of “personal information.” Pursuant to these laws, “personal information” means a state resident’s first name, or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data element is unencrypted or not redacted: (i) an SSN, (ii) a driver’s license or state identification card number, or (iii) an account number, credit or debit card number, with any required security code, access code, or password that would permit access to a resident’s financial account.⁴⁶ In many states, the definition of personal information includes the standard definition set forth above as well as numerous other data elements.⁴⁷

In addition to notification obligations imposed by state breach laws, some commentators have suggested that the ABA Model Rule of Professional Conduct 1.4 requires attorneys to notify clients of a breach of confidential information.⁴⁸ According to the commentators, notification is required because the client “ultimately will have to decide what to do about [the breach].”⁴⁹

Online Privacy

Most law firms maintain websites and collect information from website visitors. For example, visitors may provide information on a firm’s site to sign up for an electronic newsletter or a blog feed, submit an inquiry via the “contact us” form or apply for a job. An accurate, clear and complete online privacy notice conveys to online visitors that the law firm respects visitors’ privacy concerns. A privacy notice should, at a minimum, set forth (i) the types of personal information the law firm collects on its website, (ii) how the information is used, (iii) to whom it

⁴⁶ See, e.g., Del. Code Ann. tit. 6 § 12B-101.

⁴⁷ See, e.g., Cal. Civ. Code §§ 1798.29(e), 1798.82(e) (California has expanded its definition of personal information to include medical or health insurance information).

⁴⁸ See *supra* note 41. Rule 1.4, in relevant part, requires attorneys to (i) promptly inform the client of any decision or circumstance with respect to which the client’s informed consent is required by the Model Rules, (ii) reasonably consult with the client about the means by which the client’s objectives are to be accomplished, and (iii) keep the client reasonably informed about the status of the matter.

⁴⁹ See *supra* note 41.

is disclosed, (iii) how the firm protects personal information, (iv) contact information for questions or comments about the firm's information practices, and (v) an effective date.

In the U.S., federal sector-specific laws require certain types of organizations, such as financial institutions, to provide privacy notices. In addition, certain state laws, such as the California Online Privacy Protection Act, require organizations to provide privacy notices in connection with the collection, use or disclosure of personal information on their websites.⁵⁰ Aside from any legal requirement to issue an online privacy notice, a growing number of organizations view the issuance of a privacy statement as a business practice necessary to meet the expectation of website visitors. The FTC has authority pursuant to Section 5 of the FTC Act to investigate and bring enforcement actions regarding misrepresentations in privacy notices published by organizations subject to the FTC's enforcement jurisdiction.⁵¹ Accordingly, law firms should ensure that privacy and information security statements they make in their online privacy notices completely accurate.

Privacy and Information Security Requirements Outside the U.S.

Many of the countries in which U.S.-based law firms typically have offices have enacted comprehensive privacy and data protection laws. The foreign requirements often differ considerably from U.S. laws in their scope and application. Many of the foreign privacy and information security laws apply to any organization that processes personal information. In addition, foreign privacy laws may define "personal information" to include data elements that typically would not be considered personal information in the U.S. For example, in the EU, personal information includes business contact information or memberships in trade groups or political organizations. While foreign jurisdictions take a comprehensive approach to regulating privacy and information security, the data processing restrictions may vary for each type of data, such as consumer data, employee data or information about an individual's health condition, political beliefs or trade union membership, which some jurisdictions consider highly confidential.

⁵⁰ See Cal. Bus. & Prof. Code §§ 22,575–22,579.

⁵¹ See, e.g., Complaint, *In re Genica Corp.*, No. C-4252 (F.T.C. Mar. 16, 2009) (The FTC alleged that the respondents falsely stated that they took reasonable and appropriate measures to protect personal information from unauthorized access.); Complaint, *In re Premier Capital Lending, Inc.*, No. C-4241 (F.T.C. Dec. 10, 2008) (The FTC alleged that Premier violated section 5 of the FTC Act by failing to meet the terms of its own privacy policy.); Complaint, *In re Goal Fin., LLC*, No. C-4216 (F.T.C. Apr. 9, 2008) (The FTC alleged the respondent violated the FTC Act by falsely representing to consumers that it took reasonable steps to protect personal information.).

Cross-Border Transfers of Personal Information

Law firms seeking to transfer records containing personal information from a foreign jurisdiction to the U.S. should be aware of and comply with the restrictions that many countries impose on exporting personal information. Countries that have imposed such restrictions include member states of the European Union, Switzerland, Argentina, Australia, Israel, Russia, Japan, Korea and Taiwan.⁵²

Notably, some of the restrictions may have limited scope or provide for legal transfer mechanisms on which law firms and their clients may rely to transfer personal information to the U.S. For example, the European Union allows transfers of personal information only to jurisdictions that provide “adequate” privacy protection, as determined by the European Commission.⁵³ Because the Commission has not deemed the U.S. adequate (or many other jurisdictions that are important for business purposes), organizations must establish a legal basis for sending personal information from the EU to the U.S. Subject to certain exceptions, an EU entity wishing to legally transfer personal information from the EU to the U.S., may transfer the information only to a U.S. entity that has either (i) certified compliance with the privacy principles set forth in the U.S.-EU Safe Harbor Program,⁵⁴ (ii) signed model contractual clauses that contractually bind the entity to appropriately safeguard the privacy and security of personal information, or (iii) implemented binding corporate rules – a set of internal policies that prescribe certain privacy and information security measures that the entity must implement to safeguard personal information.

One of the consequences of the EU restrictions on cross-border transfer of personal information are the limitations these requirements impose on a law firm’s ability to receive in the U.S. documents containing personal information from the EU. The issue is exacerbated further by the broad interpretation of the term “personal information” under EU data protection law. For example, the inclusion under EU data protection law of business contact information within the scope of “personal information” has the potential to affect every business record originating in the EU. As a result, business records in Europe may be subject to data processing restrictions

⁵² Member states of the European Economic Area (the “EEA”) and Switzerland generally follow the EU data protection framework and, in particular, have adopted cross-border data transfer restrictions implemented in the EU.

⁵³ Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) recital 57 & art. 25(1) (the “Data Protection Directive”).

⁵⁴ See Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/eg_main_018236.asp.

that make it difficult for a U.S. entity to reach the data, for example, for purposes of litigation discovery.

Conflicting obligations of U.S. discovery rules and EU data protection laws may in turn expose law firms and their clients to a range of potential adverse consequences.⁵⁵ In the U.S., litigants who fail to comply with evidence preservation and discovery obligations are subject to a variety of sanctions. At the same time, failure to comply with EU data protection law could expose a law firm or its client to burdensome investigations, cause a disruption in the flow of personal data from the EU, and lead to enforcement by EU member states' data protection authorities. Such enforcement could result in significant fines and possible criminal penalties.

U.S. courts have shown some flexibility in considering whether a party may be excused from complying with discovery obligations that conflict with applicable foreign law. In determining whether to excuse or otherwise accommodate such noncompliance, courts consider (i) whether the information being sought originated in the U.S., (ii) the availability of alternative means to obtain the information, (iii) the extent to which noncompliance would undermine important interests of the U.S., (iv) the extent to which compliance would undermine important interests of the states in which information is located, and (v) the degree of hardship on the producing party and whether such hardship is self-imposed.⁵⁶ This is a fact-intensive inquiry the outcome of which is difficult to predict. Generally, however, courts are more sympathetic to litigants seeking discovery relief when the party has made a good faith effort to comply with their U.S. discovery obligations or where the information can be obtained through means that would not infringe competing EU legal considerations. Courts are likely to compel U.S. discovery, however, in circumstances in which the records being sought are important to the

⁵⁵ See, e.g., *U.S. v. First Nat'l Bank of Chicago*, 699 F.2d 341 (7th Cir. 1983) (vacating the district court's rejection of a foreign law defense to production of documents and ordering reconsideration of whether to require the defendants to make a good faith effort to obtain permission from Greek authorities to disclose the requested information); *Salerno v. Lecia, Inc.*, 1999 WL 299306 (W.D.N.Y. 1999) (denying motion to compel production of severance package information for defendant's European employees because disclosure of such information was prohibited under the Data Protection Directive and the requesting party did not demonstrate persuasive argument to the contrary); see also *Volkswagen v. Valdez*, 909 S.W.2d 900 (Tex. 1995) (ruling against the disclosure of a party's German corporate directory because litigants could discover the information through less intrusive means and avoid violating German privacy laws); cf. *Strauss v. Credit Lyonnais*, 2007 WL 1558567 (E.D.N.Y. May 25, 2007) (compelling discovery where defendant did not demonstrate that it would face substantial hardship if it produced the documents in contravention of French law and plaintiffs did not have any other means to obtain the requested information); *Columbia Pictures Indus. v. Bunnell*, 2007 WL 2080419 (C.D. Calif. May 29, 2007) (finding that defendants chose to locate their server in the Netherlands at least in part to take advantage of the perceived protections afforded by the country's information security law); *Remington Prods. v. North Am. Philips*, 107 F.R.D. 642, 647, 651 (D. Conn. 1985) (finding that a litigant had raised the foreign privacy law objection for the purpose of avoiding discovery rather than complying with Dutch law).

⁵⁶ See, e.g., *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for Southern Dist.*, 482 U.S. 522 (1987).

litigation and the information cannot be obtained by alternative means, or if the court finds that a party has invoked a foreign law to circumvent its U.S. discovery obligations.

Enforcement Actions for Privacy and Information Security Violations

Enforcement actions for violations of privacy or information security requirements can take a variety of forms. On the federal level, the FTC guards against unfairness and deception in organizations' privacy practices. Specifically, Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce" and authorizes the FTC to seek injunctive and other equitable relief for violations.⁵⁷ The FTC Act is the mechanism that allows the FTC to undertake enforcement actions against privacy practices that the FTC deems "unfair" or "deceptive." The "unfairness" and "deception" violations are distinct and the FTC has relied on both theories in its privacy-related enforcement.

In actions alleging deceptive practices, the FTC has pursued organizations that have misrepresented either (i) the security measures they employ to protect personal information from unauthorized access, or (ii) the manner in which the organization used or disclosed the information.⁵⁸ The FTC also has brought enforcement actions under the unfairness prong of Section 5. The unfairness theory has been used primarily to bring enforcement actions against organizations that did not make representations about the adequacy of their information security practices but, instead, suffered an information security incident that, according to the FTC, exposed the objective inadequacy of the organization's information security measures. Several FTC enforcement actions highlight this increased emphasis on the unfairness prong.⁵⁹ These cases reiterate that the FTC believes that organizations engage in unfair practices in violation of Section 5 of the FTC Act when they fail to sufficiently safeguard personal information, regardless of whether any affirmative representations regarding personal information protection were made.

The FTC has in most cases settled its privacy-related enforcement actions by consent order. In cases involving allegations of inadequate security, FTC consent orders typically

⁵⁷ 15 U.S.C. § 45.

⁵⁸ See, e.g., Complaint, *In re Geocities*, No. C-3850 (F.T.C. Feb. 5, 1999); see also Complaint, *In re Petco Animal Supplies, Inc.*, No. C-4133 (F.T.C. Mar. 4, 2005); Complaint, *In re Guess?, Inc.*, No. C-4091 (F.T.C. July 30, 2003).

⁵⁹ See, e.g., Complaint, *In re TJX Companies, Inc.*, No. C-4227 (F.T.C. July 29, 2008); Complaint, *In the Matter of Reed Elsevier Inc.*, No. C-4226 (F.T.C. July 29, 2008); Complaint, *In re CardSystems Solutions, Inc.*, No. C-4168 (F.T.C. Sept. 5, 2006); Complaint, *In re DSW, Inc.*, No. C-4157 (F.T.C. Mar. 7, 2006); Complaint, *In re BJ's Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005).

require organizations to implement comprehensive information security programs and conduct periodic compliance audits for as long as twenty years.

In addition to FTC enforcement, state laws typically give enforcement authority to state attorneys general to bring actions for unfair or deceptive trade practices on behalf of the state. Some state laws also provide for a private right of action for individuals affected by unfair or deceptive trade practices. In addition, state security breach notification laws may authorize state agencies to bring enforcement actions in connection with information security breaches and to seek civil remedies in most states.

Professional Ethics Considerations

In addition to FTC and state enforcement, law firms may face judicial sanctions for privacy-related violations of professional ethics rules. For example, in *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court held that the law firm representing the defendant employer violated New Jersey Rule of Professional Conduct 4.4(b) in reviewing the plaintiff employee's communications with her attorney.⁶⁰ The court considered whether the plaintiff had a reasonable expectation of privacy in emails she exchanged with her attorney via her web-based personal email account. Stengart used her employer-issued computer to communicate with her attorney by email. As a result, images of the emails were saved by the employer's monitoring system, which saved every web page visited on the computer. After Stengart left Loving Care and filed suit against the employer, the emails were retrieved from the laptop and the employer attempted to use Stengart's communications in the litigation. Stengart argued that the employer could neither review the emails nor use them in litigation because the email exchanges with her attorney were private and not subject to the former employer's review. The Court agreed, and held that the law firm representing the employer violated New Jersey Rule of Professional Conduct 4.4(b) by reviewing and using Stengart's communications with her attorney in the litigation.⁶¹ Rule 4.4b provides that a lawyer who receives a document, such as an email, and who has a reasonable cause to believe that the document was inadvertently sent, shall not read the document or, if the attorney has begun to do so, shall stop reading the document and promptly notify and return the document to the sender. The court did not suggest any bad faith

⁶⁰ See 990 A.2d 650.

⁶¹ ABA Model Rules of Professional Conduct serve as models for the attorney ethics rules of most states, including New Jersey. California is the only state that does not have professional conduct rules that follow the format of the Model Rules. See ABA Center for Professional Responsibility, at http://www.abanet.org/cpr/mrpc/model_rules.html.

in the way the employer's firm reviewed Stengart's attorney-client communications. Instead, the Court found that the firm erred by not setting aside arguably privileged communications once it realized they were attorney-client communications and failing to notify its adversary or seek the court's permission before reading further. Based on these findings, the court remanded the sanctions issue to the trial court to decide whether disqualification of the firm, screening of attorneys, imposition of costs or some other remedy was appropriate under the circumstances.

Future Trends in Privacy Regulation

Privacy law in the United States and throughout the world continues to evolve. In the U.S., lawmakers are seeking to enact legislation that will address privacy and information security in a comprehensive manner. For example, on July 22, 2009, Senator Patrick Leahy reintroduced a privacy bill that includes federal data security breach notification requirements.⁶² The Personal Data Privacy and Security Act would require entities engaged in interstate commerce to notify individuals if certain of their computerized personal information is subject to a data security breach. The proposed bill also would require organizations that collect, use or access the sensitive personally identifiable information of more than 10,000 individuals to implement a comprehensive data security and privacy program. The notification provisions of the proposed law would effectively preempt state breach notification laws. The bill also seeks to enhance the FTC's enforcement authority by empowering the agency to (i) undertake enforcement actions against practices the FTC deems harmful to consumers, irrespective of whether such practices could be construed as unfair or deceptive, (ii) impose civil penalties for violations, and (iii) promulgate enforceable regulations establishing standards for data security.

Privacy legislation also has been introduced in the House of Representatives. On May 4, 2010, Congressmen Rick Boucher and Cliff Stearns introduced bipartisan draft legislation designed to protect the privacy of personal information both on the Internet and offline.⁶³ The proposed legislation would apply to any organization engaged in interstate commerce that collects personal information. The bill would require covered entities to (i) provide individuals with a privacy notice and, subject to certain exceptions, an opportunity to opt out before the organization may collect, use or disclose the individual's personal information, (ii) obtain the opt-in consent of individuals before collecting sensitive information such as medical or financial

⁶² Personal Data Privacy and Security Act of 2009, S.1490, 111th U.S. Congress (2009-2010), <http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:./temp/~bdyTMX:@@L&summ2=m&/bss/111search.html>.

⁶³ A staff discussion draft of the proposed legislation is available at http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf (last visited May 17, 2010).

records, (iii) obtain the opt-in consent of individuals before sharing personal information with unaffiliated parties, and (iv) establish, implement and maintain appropriate administrative, technical and physical safeguards to protect covered information. The draft legislation would give enforcement authority in the FTC as well as state attorneys general and state consumer protection agencies.

While data protection law in the EU is more comprehensive than in the U.S., EU member states have not, until recently, enacted comprehensive breach notification legislation. For example, on February 24, 2010, the French Senate published an amended bill on the right to privacy in the digital age.⁶⁴ Among the many amendments, organizations with more than fifty employees accessing or processing personal data would be required to appoint a data protection officer (“DPO”). The DPO would play a central role in the handling of information security breaches and maintain an inventory of all data security breaches suffered by the organization. In the event of an information security breach, the organization that is the data controller would be required to inform the DPO of the breach or, in the absence of a DPO, the French data protection authority. Under the proposed bill, upon discovering a breach, the DPO would be required to take all necessary measures to (i) restore the integrity and confidentiality of the data, and (ii) notify the French data protection authority of the incident.

Breach notification legislation is also under consideration in Australia. The Australian Law Reform Commission recently promulgated a report that included a recommendation that the Australian government introduce mandatory information security breach disclosure laws.⁶⁵ The report suggested that the government adopt a notification scheme that does not apply to all potentially “trivial breaches.” Rather, the recommendation calls for a disclosure requirement in circumstances in which an information security breach could result in “serious harm” to affected individuals.

Finally, some countries that previously had weak or limited privacy regimes have accelerated efforts to enact omnibus data protection legislation. For example, Taiwan recently has expanded the scope of its comprehensive data protection law to apply to private entities. In addition, a data protection bill has been tabled in Singapore, and data protection bills in Mexico and Malaysia have been approved by legislatures and are slated to be signed into law.

⁶⁴ See Proposition de loi visant à mieux garantir le droit à la vie privée à l’heure du numérique, adoptée par le Sénat le 23 mars 2010, at <http://www.senat.fr/leg/tas09-081.html>.

⁶⁵ Australian Law Reform Commission, ALRC Report 108 For Your Information: Australian Privacy Law and Practice, Ch. 51 (30 May 2008).

Conclusion

The requirements described in this article represent only the tip of the iceberg when it comes to privacy and information security issues that a law firm should consider. For law firms, it is difficult to overemphasize the importance of (i) understanding how the firm collects, uses and otherwise processes personal information, (ii) thoroughly analyzing the firm's relevant legal obligations, and (iii) implementing a comprehensive privacy and information management strategy to address these obligations.

Law firms should expect that they will face increasing attempts by unauthorized persons to gain access to information that they maintain, including personal information. One of a law firm's greatest assets – its reputation – is threatened by the possibility of a breach that ruins a deal or embarrasses a client. A simple misstep in the safeguarding of personal information can lead to far-reaching and expensive consequences, including the loss of revenue and client trust. Accordingly, law firms would be well-served to take a proactive approach to privacy and information management by voluntarily implementing comprehensive measures to protect the security, confidentiality and integrity of personal information. The most successful programs will include administrative, technical and physical safeguards to protect personal information, and should be subjected to periodic internal testing. While the creation of a privacy and information security program may seem like a daunting task, such measures can help prevent the occurrence of a high-profile, embarrassing and costly privacy and information security incidents.



www.hunton.com

Atlanta Austin Bangkok Beijing Brussels Charlotte Dallas Houston London Los Angeles

McLean Miami New York Norfolk Raleigh Richmond San Francisco Washington



The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2010 CNA. All rights reserved. RiskPerInfoHunton710