4-19-2015

Data Breaches and Privacy Law: Lawyers' Challenges in Handling Personal Information

Charlotte Duc-Bragues
Cornell Law School

Law and Technology – Spring 2015

Charlotte Duc-Bragues, J.D.-Maîtrise Candidate 2015

Data Breaches and Privacy Law: Lawyers' Challenges in Handling Personal Information

"*The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability*."

(Leon Panetta, former CIA director and current U.S. Secretary of Defense[1])

Sharing personal information with a lawyer potentially represents the greatest source of vulnerability for an individual. Since the first major security breach in 2005, law firms have been pressed both by public authorities and clients to take action in order to protect confidential information from potential harmful breaches[2].

This paper seeks to provide an overview of the challenges faced by lawyers in handling personal information with regard to potential security breaches. The aim is to analyze this issue through the focal of privacy law; statistics on security breaches and tools to prevent this phenomenon, extensively studied in class, are given less attention.

I. Growing Need to Protect Clients' Personal Information

a. Escalating trend of security breaches and concerns over the protection of sensitive personal data

Prevalence of Security Breaches – It is hard to gauge the extent to which law firms are vulnerable to attacks form hackers, mainly because law firms maintain a lead blanket and underreport cybersecurity breaches by fear of repercussion on their reputation[3]. Yet, numerous reports have provided evidence of a growing number of data breaches and showed that law firms had become "particularly attractive targets."[4] Over the last several years, "the frequency of data security breaches [in all economic sectors] has skyrocketed," with reports establishing its figure at more than 600 million since 2005[5]. Since 2010, data breaches have reached new records: between 2010 and 2012, 800 breaches have been reported, a substantial increase from the 900 incidents that had reported between 2005 and 2010[6]. In 2011, 80 out of the 100 major law firms have had "malicious security breaches"[7] and in 2012, 10% of the cyberattacks were directed at law firms. Professionals in the information security sector ironize today that question seems no longer to be "whether" law firms are going to be hacked, but "when."[8]

Concerns over Protection of Sensitive Personal Data – Hackers infiltrate law firms not only to obtain sensitive material related to negotiation positions, business strategies, or clients' transactions, but also

personal information about a law firm's client or employee[9]. Among the various motives of hackers, the breach of personal sensitive data constitutes a violation of personal privacy that is of the utmost concern. It might result in "immediate and immeasurable injury," such as harm to the person's reputation and financial security[10], as well as a greater risk of future identity theft[11].

b. Defining "Personal Information"

Absence of uniform definition – Unlike the European Union, the U.S. does not have a uniform definition of "personal data" and instead has adopted a sectorial approach to defining and regulating privacy[12]. Consequently, state and federal laws provide different definitions of "personal information" (see infra, Part II).

FTC's definition seen as the most relevant – Usually[13], two labels encompass the notion of sensitive personal information: (i) personally identifiable information (PII), and (ii) protected health information (PHI). The definition of PII most widely used by law firms is the one applied by the FTC in its privacy and information security enforcement actions under Section 5 of the FTC Act[14]. The federal agency defines personal information as "individually identifiable information that is from or about an individual including, but not limited to" a list of computerized data, which includes a person's: (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; (d) a telephone number; (e) a Social Security number; (f) a driver's license number; (g) a credit card or debit card account number; (h) a persistent identifier, such as a customer number held in "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information that is combined with any of (a) through (h) above.[15] However, the definition of personal information is "a moving target," in that it is "difficult if not impossible to establish a finite set of data elements that can identify an individual and, therefore, warrant legal protection," as the FTC has warned in the past when it released a report on self-regulatory principles for online behavioral advertising[16].

Threefold nature of the risk of mishandling personal information – There are three broad categories of breaches that can expose private electronic data: (i) careless disposal of client records, (ii) theft of mobile device, and (iii) misuse of security protocols.[17] The numerous circumstances from which that risk may arise stem from the various roles of a law firm: as an employer, the law firm handles personal information of employees' (e.g., employees' payroll or retirement plan); as a provider of legal services the law firm receives information from clients; as a litigator, the law firm receives files obtained through discovery; also, a law firm routinely allows third parties to access to personal information (*e.g.*, when third party vendor helps processing clients' files).

II. Current Legal Framework on Data Security and Privacy Affecting Law Firms

There is no comprehensive data privacy or security law framework at the federal level. As a result, obligations binding on lawyers in this realm stem from three sources: ethical, common law, and regulatory.

a. Ethical obligations

When handling personal information, lawyers must abide by the duty of competent representation cover by ABA Model Rule 1.1 and the duty of confidentiality defined by ABA Model Rule 1.6, and especially be aware of Comment 16 to this latter rule that requires them to take reasonable precautions to safeguard and preserve confidential information against inadvertent disclosure such as in the case of cybersecurity breach (it has become clear that rules applies equally to electronic data on computers and on paper format[18]).

b. Common law obligations and State Law Requirements

Duties at common law are parallel to ethical duties mentioned above[19]. Equally important, most states either have general security laws or laws that require specific safeguards generating the obligation for lawyers to develop and maintain "reasonable measures" to protect categories of personal information (they vary among states but the categories defined by the FTC and enumerated above are the ones usually retained by states too[20]). The fundamental challenge for lawyers is then to determine what the standard for

"reasonable measures" encompasses (as discussed in Part III below). Last but not least, in addition to and more prevalent than ex-ante obligations, almost all the states have passed laws requiring notification following data breaches (46 states have such requirement to date[21]). They generally require law firms that possess categories of PII as defined by state law to notify affected employees or clients.

c. Regulatory obligations and Government Enforcement of Data Security and Privacy Laws

Despite the lack of comprehensive federal law governing this issue, there are, however, federal laws that apply to specific industries as a result of the U.S. following a "sectorial" approach to security breaches. Hence, law firms victim of hackers' attacks have to comply with the requirements found in the specific statute governing the sector in which their client operate[22]. In addition to these federal requirements, the FTC takes enforcement actions, under Section 5 of the FTC Act, against organizations whose privacy or information security practices it deems unfair or deceptive. Yet, law firms have been exempted from the Title V of the Gramm Leach Bliley Act of 1999 (GLBA), which is the major statute gathering privacy and security laws that applies to financial institutions. Courts have considered that law firms are neither "financial institutions" within the meaning of GLBA, nor subject to statutes implemented by the FTC, such as the Identity and Theft Red Flags Rule[23]. As a result, these exemptions might be seen as lifting the pressure on law firms to comply with regulations' information security and privacy requirements designed to prevent data breaches.

III. Preventing Data Breaches

a. Three Major Obstacles

Invisibility of Computer Data Theft – When data is stolen, most of the time the victim of the attack does not realize it because the data is copied and does not disappear from the victim's computer. Practice shows that major law firms victim of data security breach either do not know it or discover it months later.

Cost and Inconvenience of Security Programs – Implementing strong security programs requires hiring IT staff, buying software, training employees, and ensuring compliance with professional standards, which altogether amounts to costly spending for law firms. Moreover, requirements imposed on lawyers personally (such as, inter alia, changing passwords, not carrying sensitive data on mobile devices) can represent an overwhelming day-to-day hassle for them.

Law Firm's Culture – Starting in 2011, the Federal Bureau of Investigation has been acting to press law firms to take data security threats seriously[24]. Law firms, even after being warned by the FBI, consider these threats as "overstated." (see Goldstein). Indeed, studies show that many partners lack interest in data security, thus making it "socially and culturally difficult to impose [security] policies."[25]

b. "Reasonable Measures" to Prevent Data Breaches

General Frameworks – Acknowledging that the core challenge for lawyers is to determine what "reasonable measures" mean (see Part II supra), the ABA recommends lawyers to follow the FTC's "Safeguard Rules" under the GLBA, as well as the standards suggested by the International Organization for Standardization (ISO). These sources provide altogether a comprehensive framework of components necessary for a "complete security program."[26]

Preventing Data Breaches in Practice – A recent trend shows that law firms are more disciplined in providing security programs. Both federal and state statutes seem to have pushed them towards structuring information security programs in three steps[27]: (1) establishing security objectives; (2) identifying security needs; and (3) implementing a security program[28].

To conclude, in addition to ethical duties that can make them subject to discipline, lawyers have to comply with requirements that exist both at the state and federal levels. However, the main source of incentive in the future for law firms to implement security programs is more likely be the pressure from clients to have their personal information protected.[29]

APPENDIX 1: Checklist for Monitoring Where PII or Personal Information is Stored

PII OR PERSONAL INFORMATION TYPE IN COMBINATION WITH FIRST NAME OR FIRST INITIAL AND LAST NAME	ENCRYPTION		LOCATION								
	ENCRYPTED	ENCRYPTION KEY NOT WITH DATA	DO NOT COLLECT	NETWORK	LAPTOP	USB DRIVE	E-MAIL	BLACKBERRY OR PDA	CELL PHONE	COMPUTER HARD DRIVE	CD OR DVD
Address and telephone number (by itself it is not considered a breach because of its availability in public records)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Driver's license or state personal identification card number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Social Security Number (SSN)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Place of employment	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Employee identification number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Employer or taxpayer identification number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Government passport number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Health insurance identification number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Mother's maiden name	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Demand deposit account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Savings account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Financial transaction device account number or the individual's account password	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Stock or other security certificate or account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Credit card account number	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Vital record	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Medical records or information	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Demand deposit or other financial account number, or credit card or debit card number in conjunction with any required security code, access code, or password that would permit access to any of the individual's financial accounts	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒

[1] Leon E. Panetta, Sec'y, U.S. Dep't of Defense, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), available at http://www.defense. gov/ transcripts/transcript.aspx?transcriptid=5136.

[2] Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. (2013), at 1368.

[3] "Few law firms will admit publicly to a breach (…) Thefts of confidential information strike at the core of the legal profession's obligation to safeguard clients' secrets, and can do considerable harm to a firm's reputation," in "Lawyers Get Vigilant on Cybersecurity," Jennifer Smith, in The Wall Street Journal, June 26, 2012.

[4] Alan Ezekiel, "Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft," 26 Harvard Journal of Law & Technology 649, 2013.

[5] Carolyn A. Deverich et al., *Into the Breach*, L.A. LAW., Feb. 2012, at 2.

[6] Miles L. Galbraith, Comment, Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information, 62 AM. U. L. REV. 1365, 1399 (2013). Internet Crime Complaint (13)

[7] CNA PROFESSIONAL COUNSELSM – Safe and Secure: Cyber Security Practices for Law Firms (https://www.cna.com/web/wcm/connect/61aec549-ac28-457b-8626-aa791c782459/Safe_Secure_Cyber_Security_Practices.pdf?MOD=AJPERES)

[8] *Id*.

[9] Carolyn A. Deverich et al., *Into the Breach*, L.A. LAW., Feb. 2012, at 2.
[10] TJX Company exposing 95 million customers' credit and debit card account numbers. See Miles L. Galbraith, supra note 5.
[11] See Carolyn A. Deverich, supra note 4.
[12] Paul M. Schwartz and Daniel J. Solove, "Defining Personal Data in the European Union and U.S.," in *Privacy & Security Law Report*, 13 PVLR 1581, 09/15/2014.
[13] Peter Arant, "Understanding Data Breach Liability: The Basics Every Attorney Should Know." 40 Montana Lawyer 8 (Feb. 2015).
[14] Lisa J. Sotto, Aaron P. Simpson, & Boris Segalis, Law Firms Face Risks in Handling Personal Information, HUNTON & WILLIAMS LLP, http://www.cnapro.com/pdf/LawFirmsFaceRisksHandlingPersonalInformation%20(HuntonWilliams).pdf
[15] Agreement Containing Consent Order at 2, In re Dave & Buster's Inc., No. 0823153 (F.T.C. March 25, 2010).
[16] See Sotto, Simpson, and Segalis, supra note 13 at p.4.
[17] For more developments on the three major categories of data breaches involving law firms, see See Matthew H. Meade, Lawyers and Data Security: Understanding a Lawyer's Ethical and Legal Obligations that Arise from Handling Personal Information Provided by Clients, 28 Computer & Internet Law. 1, 1 (2011).
[18] David G. Ries, "Safeguarding Confidential Data: Your Ethical and Legal Obligations", ABA Law Practice (July/August 2010, Vol. 36, No. 4, at 49).
[19] See the Restatement (Third) of the Law Governing Lawyers (2000) that summarizes the common law duties relevant for the present analysis of the handling of personal information by lawyers.
[20] See Sotto, Simpson, and Segalis, supra note 13, p.2.
[21] See Ries, supra note 17, Part III, "Laws and Regulations Covering Personal Information."
[22] The major sectorial regulations include: the Electronic Communications Privacy Act ("ECPA") which governs the interception and review of electronic and wire communications; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which regulates privacy and data security issues related to PHI; the Fair Credit Reporting Act ("FCRA"), which covers information security, identity theft, and the use and disclosure of consumer reports.
[23] See Sotto, Simpson, and Segalis, supra note 13, p.3.
[24] The federal agency has indeed held meetings with managing partners practicing law in major U.S. cities to warn them on the issues of computer security and corporate espionage, and especially those having offices in countries such as China or Russia. See M. Goldstein, "Law Firms Are Pressed on Security for Data," in *The New York Times*, March 26, 2014.
[25] See Ezekiel, supra note 3, Part II.D.
[26] See Ries, supra note 17, Part III, "Laws and Regulations Covering Personal Information."
[27] See David Z. Bodenheimer and Cheryl A. Falvey, "Cybersecurity Standards and Risk Assessments for Law Offices: Weighing the Security Risks and Safeguarding Against Cyber Threats," (Aug 10, 2013) Crowell & Moring. http://www.crowell.com/files/Cybersecurity-Standards-and-Risk-Assessments-for-Law-Offices.pdf
[28] See Appendix 1 for a concrete illustration of a crucial step in implementing security programs, which is monitoring where PII is stored. Real example of form provided by an information security firm. See Faith M. Heikkila, Data Privacy in the Law Firm, 88-JUL Mich. B.J. 33 (2009).
[29] See Goldstein, supra note 23.

Filter

Date	Activity	Duration	Rate	Total	Status	User
04/19/2015	Finalizing	1.2	$250.00/hr	$300.00	Open	Charlotte Duc-Bragues
04/09/2015	Writing	1.3	$250.00/hr	$325.00	Open	Charlotte Duc-Bragues
04/07/2015	Writing First Draft/Researching	8.7	$250.00/hr	$2,175.00	Open	Charlotte Duc-Bragues
04/06/2015	Drafting	1.2	$250.00/hr	$300.00	Open	Charlotte Duc-Bragues
04/02/2015	Drafting	2.5	$250.00/hr	$625.00	Open	Charlotte Duc-Bragues
03/18/2015	Research	1.1	$250.00/hr	$275.00	Open	Charlotte Duc-Bragues
03/17/2015	Research	0.3	$250.00/hr	$75.00	Open	Charlotte Duc-Bragues
03/17/2015	Research	2.0	$250.00/hr	$500.00	Open	Charlotte Duc-Bragues
02/20/2015	Research	4.0	$250.00/hr	$1,000.00	Open	Charlotte Duc-Bragues
02/06/2015	practice billing	4.9	$250.00/hr	$1,225.00	Open	Charlotte Duc-Bragues