Antitrust, Vol. 28, No. 3, Summer 2014.

Moving Target: Protecting Against Data Breaches Now and Down the Road

BY DANA ROSENFELD AND DONNELLY McDOWELL

IN THE WAKE OF A NUMBER OF HIGH-profile and high-impact data breaches, the patchwork of federal and state laws and regulations governing data security is generating more interest than ever. As federal and state regulators debate whether and how laws should be changed, consumers and financial institutions have attempted to work within the existing legal framework to impose liability upon retailers for data breaches. Meanwhile, companies that store consumer information are wondering how these developments should impact their data security practices.

This article begins by exploring the current legal and regulatory landscape governing data security and data breaches, including recent enforcement actions. We then examine some notable proposals to amend existing laws and discuss what companies should be doing now, both under existing law and to prepare for potential changes down the road.

Current Legal and Regulatory Landscape

Although companies often find it most efficient to treat all data, or at least all sensitive data, in the same manner, there is no single legal standard governing data security and thus a single company's data may be subject to different obligations under various federal and state laws. Depending on such factors as the type of information, where the information is stored, how it is stored, and who stores it, a company's data security practices may be subject to distinct but overlapping requirements. Such requirements relate to aspects such as usage, third-party sharing, security and compliance mechanisms, and what to do in the event of a breach.

Dana Rosenfeld is a partner in Kelley Drye's Washington, D.C. office and chair of the Privacy and Information Security practice. A former assistant director of the FTC Bureau of Consumer Protection, Ms. Rosenfeld focuses her practice on privacy and data security, advertising, and consumer financial issues at the federal and state level. Donnelly McDowell is an associate in Kelley Drye's Washington D.C. office and part of the firm's Advertising and Marketing and Privacy and Information Security practice groups.

Federal Law. Companies collecting and storing consumer information for commercial uses must comply with a host of federal laws targeting use and collection of certain particularly sensitive information, along with general standards imposed by the Federal Trade Commission under the FTC Act.[1] For instance, the Gramm-Leach-Bliley Act (GLB Act) requires financial institutions to protect consumers' nonpublic personal information, including by preventing disclosure to unauthorized third parties.[2] As part of its implementation of the GLB Act, the Commission promulgated the Safeguards Rule, which requires subject entities to develop a written information security plan describing their program to protect consumer information. The written plan must, *inter alia*, "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in [its] unauthorized disclosure."[3]

Entities that use or provide consumer reports must also comply with the Fair Credit Reporting Act (FCRA), which requires consumer reporting agencies to, among other things, "maintain reasonable procedures designed to avoid" disclosing consumer information and imposes safe disposal obligations on entities that maintain or otherwise possess information used in consumer reports.[4] Regulations implementing the safe disposal obligations provide that reasonable measures include, but are not limited to, "[i]mplementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed."[5]

While the GLB Act and FCRA only apply to certain entities and to certain types of information,[6] the FTC Act and the Dodd-Frank Act[7] provide the FTC and the Consumer Financial Protection Bureau (CFPB), respectively, with broader authority to regulate certain acts and practices as "unfair" or "deceptive." In the data security context, the FTC has used this authority to allege that a company committed a deceptive act where it made materially misleading statements or omissions regarding the security provided for consumer information. For instance, in an action brought against mobile phone manufacturer HTC America Inc., the FTC alleged that HTC engaged in deceptive acts by representing that users would be notified when a third-party application sought access to the their stored information when, in fact, third-party applications could access information without notification or consent due to security vulnerabilities.[8] Similarly, HTC also allegedly misrepresented that it would not collect user location data unless users opted in to sharing such data when submitting complaints through the company's "Tell HTC" application.

Wyndham and LabMD Cases. In addition to the FTC's use of its authority to prevent deceptive acts and practices, the Commission has also brought data security actions using its unfairness authority when it has determined that a practice is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and is not

outweighed by countervailing benefits. Notably, Wyndham Worldwide and LabMD have recently challenged the FTC's authority to regulate data security practices as unfair under the FTC Act.[9] In both cases, the FTC alleged that the companies engaged in unfair practices by failing to employ reasonable and appropriate measures to prevent unauthorized access to sensitive consumer information.[10]

In the administrative complaint against LabMD, the FTC alleged that the company's use of a peer-to-peer file-sharing network unreasonably exposed sensitive consumer information, including health information, to unauthorized access. Similarly, the Commission's federal court complaint against Wyndham asserted that the latter engaged in unfair practices by failing to take a variety of precautions at independently-owned Wyndham-branded hotels to protect consumer information, including failing to employ firewalls and network segmentation between the Wyndham-branded hotels and the corporate network. Such failure, the complaint alleged, allowed software to be configured inappropriately, and failed to require complex user IDs and passwords to prevent hacking.

Following the issuance of the FTC complaint, Wyndham filed a motion to dismiss alleging that the FTC lacked authority to use its unfairness authority in the data security context. Wyndham also asserted that the FTC must formally promulgate rules before bringing an unfairness claim in the data security context and that its failure to do so violated fair notice principles.[11] In further support of this argument, Wyndham later pointed to recently introduced Senate bills that would require the FTC to establish standards through notice-and-comment rulemaking, rather than through exercise of enforcement discretion and the issuance of consent orders.[12]

On April 7, 2014, the New Jersey District Court issued an opinion, ruling on Wyndham's motion to dismiss, finding for the FTC on all grounds.[13] Notably, the court found no "carve out [for] a data security exception to the FTC's authority," although it emphasized that a "liability determination is for another day" and that its decision "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked."[14]

The court concluded that the FTC's unfairness authority over data security practices coexists with its data security authority under the current regulatory scheme. In addition, the court found that data security legislation proposed by Congress, and the FTC's public representations that it lacks the authority to require entities to adopt privacy policies, do not give rise to a data security exemption from the FTC's unfairness authority. The opinion recognized that previous circuit courts of appeal decisions have affirmed FTC unfairness actions in a variety of contexts without preexisting rules or regulations specifically addressing the conduct at issue. The court was also unpersuaded that regulations are the only means of providing sufficient fair notice, and stated that Wyndham's "argument that consent orders do not carry the force of law . . . misses the mark." Indeed, the court found that FTC's rulings, interpretations and opinions, while not controlling upon the courts, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance.

Wyndham further argued that an unfair practice must, by statute, cause consumer injury, and that injury from theft of payment card data is never substantial and always avoidable. The court, however, found that the FTC's complaint sufficiently pled an unfairness claim under the FTC Act. Importantly, the court stated that the FTC's allegations permit it to reasonably infer that Wyndham's data security practices caused theft of personal data, which caused substantial injury to consumers.

Lastly, in finding that the FTC's deception claim was sufficiently pleaded, the court turned to the specific language of Wyndham's privacy policy. Wyndham argued that its privacy policy specifically excludes Wyndham-branded hotels from the policy's data-security representations. The court was not convinced, noting that a reasonable customer would have understood that the policy makes statements about data-security practices for both Wyndham and Wyndham-branded hotels.

As in Wyndham's case, LabMD has been unsuccessful thus far in its challenges to the FTC's authority to regulate data security practices as unfair. On May 12, 2014, the District Court for the Northern District of Georgia denied LabMD's motion for a preliminary injunction to enjoin the Commission's enforcement action on ripeness grounds because, according to the court, the Commission had yet to take final action subject to review under the Administrative Procedure Act.[15] While both Wyndham and LabMD have been unsuccessful in their challenges to FTC authority thus far, both those decisions are being appealed and both cases therefore warrant careful monitoring. However, at least pending the resolution of those challenges, companies should consider the FTC's use of its deception and unfairness authority as another piece in the mosaic of the data security legal framework. Indeed, the FTC has brought more than 50 actions alleging that a company's data security practices were unfair or deceptive, as discussed below.[16]

State Law. In addition to federal law, state law imposes another layer of data security requirements on entities that collect and maintain consumer information. Some states have general data security laws in place that require businesses to act reasonably to ensure that consumer information is maintained safely within their custody and not susceptible to breach.[17] In addition to imposing a general obligation to implement and maintain reasonable security procedures and practices, those laws may impose more specific obligations, such as requiring third parties by contract to protect personal information to the same extent as the business,[18] prohibiting retention of payment information such as security code data or the PIN verification code,[19] requiring businesses to encrypt personal information when transmitted over

Given the lack of a federal data breach law covering personal consumer information generally, states presently impose the first and most direct legal requirements for notification when a data breach occurs. To date, 46 states and the District of Columbia have data breach notification laws in place.

public networks or stored on portable media,[20] or requiring businesses that accept payment cards to comply with the most current version of the Payment Card Industry Data Security Standard (PCI DSS).[21]

For example, Massachusetts law, which is more extensive than that of any other state, imposes a series of requirements on any company that stores personal information regarding a Massachusetts resident. Those requirements include maintenance of a comprehensive information security program that contains administrative, technical, and physical safeguards and granular computer security requirements such as secure user authentication protocols, secure access control measures, and encryption of all transmitted records or records stored on laptops or other portable devices.[22]

A larger proportion of states do not have laws directly regulating general data security practices on their books, but do employ other laws regulating the collection and treatment of particularly sensitive information like social security numbers. Of course, even strict compliance with the most stringent data security laws may not be sufficient to protect against data breaches. Some have questioned the utility of specific standards like the PCI DSS, given that large retailers like Target and Neiman Marcus suffered breaches notwithstanding having obtained certifications for compliance with the standard.

On the opposite side of these state safeguard laws, there are laws that govern what an entity must do in the event of a customer data breach. Given the lack of a federal data breach law covering personal consumer information generally,[23] states presently impose the first and most direct legal requirements for notification when a data breach occurs. To date, 46 states and the District of Columbia have data breach notification laws in place. Although state data breach laws generally require entities to provide notification when unauthorized access to or acquisition of sensitive personal information has taken place, the laws vary in several important respects, including what constitutes sensitive personal information, the degree of investigation required after a breach, who must be notified, and how they must be notified.

For larger data breaches, multiple state laws will likely be implicated in some respect, because the laws often apply based on the residency of the consumer rather than the location of the data. In some respects, this is problematic due to the aforementioned variation in the scope and requirements of the laws. On the other hand, many of the requirements are similar enough so that, depending on the scope of the breach, it may often be preferable to simply assume that a breach response will require compliance with every state law.

Current Enforcement Environment. As explained by FTC Chairwoman Edith Ramirez in recent testimony before the Senate Committee on Homeland Security and Governmental Affairs, the Commission "conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[24] For instance, the FTC recently settled charges against a provider of medical transcript services for failing to provide adequate data security measures and thus unfairly exposing sensitive consumer information including medical histories and examination notes.[25]

In a similar action, the FTC alleged that a service provider to hospitals failed to offer reasonable and appropriate security measures by transporting laptops containing personal information without adequate security, failing to adequately restrict access to consumer information, and failing to ensure that employees removed from their computers personal information that was no longer necessary for the business to maintain.[26] Actions involving the failure to limit access based on employee need and timeframe are common in FTC actions involving data security practices.

The Commission has placed particular focus on mobile data security in recent months, bringing separate actions against Credit Karma and Fandango for misrepresenting the security of mobile apps and failing to secure sensitive personal information collected by the apps. According to the complaints, both Credit Karma and Fandango failed to validate Secure Sockets Layer (SSL) certificates, which verify that a consumer's connection is authentic and secure, and therefore risked exposure to "man-in-the-middle-attacks" whereby a hacker could use spoofing techniques to access consumer payment information.[27] Notably, neither company actually experienced a reported breach and thus the cases demonstrate that companies may be at risk for FTC enforcement action even where consumer information is not actually misappropriated.

State attorneys general are more likely to bring enforcement actions in response to specific incidents, although preemptive actions are certainly possible. The Vermont Attorney General, for example, recently settled an action against Natural Provisions Inc., in which Vermont alleged that the grocer failed to take prompt remedial action after it learned of a breach involving consumers' credit cards.[28]

Companies may also face private actions under state consumer protection laws or state data security laws conferring a private right of action. For example, following a December

2013 security breach, Target now faces at least 33 actions spanning 18 districts, which were recently consolidated by the U.S. Judicial Panel on Multidistrict Litigation. The FTC has also confirmed that it is investigating whether to bring an action against Target, so the class actions may be just the tip of the iceberg for Target's legal concerns.[29]

The cases against Target are still pending, and similar class actions have had varied success in surviving motions to dismiss based on a lack of standing or a failure to demonstrate actual injury-in-fact. The Ninth Circuit, for example, permitted a suit against Starbucks to continue upon finding that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[30] However, other courts have been reluctant to find a sufficient injury-in-fact based on exposure of sensitive information through a data breach on the grounds that increased risk of injury in and of itself is too speculative to confer standing.[31] The likelihood of dismissal on standing grounds will depend on the information exposed, evidence of access, and likelihood of future use, among other factors. Even if private actions are eventually dismissed, the cost of defending against such litigation is substantial and provides another reason why companies should exercise caution in devising their data security policies and practices.

A Moving Target? What's Next?

It remains to be seen whether the recent breaches will lead to new legislation or enforcement remedies. Congress is presently considering various data breach bills that could create uniform breach notification laws and prescribe general data security and notification requirements and direct the FTC to promulgate more detailed regulations. For instance, S. 1976 would require the FTC to promulgate regulations within one year "to require each covered entity that owns or possesses data containing personal information . . . to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information."[32] In contrast, S. 1927 would direct regulations to be promulgated within six months regarding notification procedures, but arguably not require regulations regarding an entity's initial information security practices.[33] Another pending Senate bill would establish detailed data security and notification requirements, and permit enforcement by state attorneys general and individual consumers through private civil actions.[34]

Even if a federal bill specifically addressing data security fails to pass, it is possible that changes to existing legal authority could derive from more general legislation. Chairwoman Ramirez recently renewed arguments for Congress to confer the FTC with rulemaking authority under the Administrative Procedure Act.[35] While such legislation would not be directly related to data security, it would provide the Commission with new tools that it likely would use to bolster existing data security enforcement.

It is also possible that Congressional interest will fade and the current legal landscape will remain intact. Even if that occurs, however, there is little doubt that federal and state enforcement agencies will continue to make data security a priority and use existing authority to adopt new initiatives as necessary to address new and emerging risks.[36]

What Now? General Best Practices for Today

Although it is impossible to predict whether and how the legal and regulatory landscape could change in response to the recent breaches, it is clear that exposure to risk as a result of data breaches is higher than ever. Companies should make sure they have comprehensive data security and incident response plans in place that account for the patchwork of state and federal laws governing data practices. Such policies should take into account the type of data stored, the mechanisms for storage, and the duration of storage, among other factors.

There is no single "correct" data security plan as companies should adapt their policies and practices to the practical realities presented by their business model as well as the unique legal obligations affecting their industry and the type of customer information they collect and store. Nonetheless, at a minimum, we recommend that companies storing personal information consider the following key principles when devising or re-assessing their data security practices.

Do they really need it? Determine whether access to personally identifiable information is limited to those who have a valid business use for the information. Access to sensitive consumer information should be subject to particularly stringent safeguards and limited to employees who have been trained on data security issues. Along those lines, when practicable companies should avoid providing generic usernames and passwords where those provide access to consumer information. If employees do not need to use consumer information for their job responsibilities, then they should not have access to that information as a general matter.

Use it and lose it. Once consumer information is no longer needed, it should be properly disposed of, consistent with applicable laws and standards governing data destruction. Even if a company takes all reasonable steps to prevent a data security incident, it may still face liability in the event of a breach if its purpose for retaining the information had long ago passed.

What's new? Companies should stay abreast of the dynamic landscape affecting data usage, monitoring and protection, and employ industry best practices whenever possible. The more sensitive the information, the greater the need to use the most advanced and reliable technologies to secure that information.

See something? Do something about it. Companies should have active monitoring and oversight activities to ensure that data remain secure. Oversight activities should include monitoring for red flags and irregularities and conducting further inquiry as necessary when such irregularities arise. As a pre-

liminary matter, companies should have in place existing policies setting forth preliminary plans of action for possible breaches. If a breach is discovered, companies should contact counsel to determine the best course of action for that particular breach.

Conclusion

The stakes for data security are higher than ever, both from a practical standpoint to protect against bad publicity in the event of a breach, and as a legal matter to avoid enforcement or consumer class actions. Much may change in the coming months, but for now at least, companies should ensure that they have in place reasonable policies and practices consistent with the patchwork of laws governing data security. ■

[1] 15 U.S.C. § 45(a).

[2] 15 U.S.C. § 6801.

[3] 16 C.F.R. § 314.4(b).

[4] 15 U.S.C. §§ 1681e(a), 1681w.

[5] 16 C.F.R. § 682.3(b)(2).

[6] 15 U.S.C. § 6802(a) (imposing limits under the GLB Act on the disclosure of nonpublic personal information by financial institutions); 15 U.S.C. § 1681a (f) (defining "consumer reporting agency" for the purposes of the FCRA).

[7] 12 U.S.C. § 5531(a). Additionally, the CFPB has authority under the Dodd-Frank Act to take action to prevent "abusive" acts and practices, which is defined to include any act or practice that takes unreasonable advantage of a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service. Id. To date, the CFPB has not used this authority in the data security context.

[8] Complaint, HTC America Inc., FTC File No. 122 3049 (July 2, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf.

[9] Complaint, LabMD, Inc. v. FTC, No. 14-0810 (N.D. Ga. Mar. 20, 2014); Defendant's Motion to Dismiss, FTC v. Wyndham Worldwide Corp., No. 12-1365 (D. Ariz. Aug. 27, 2012).

[10] Complaint, LabMD, Inc., FTC File No. 102 3099 (Aug. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf; Complaint, Wyndham Worldwide Corp., FTC File No. 102 3142 (June 26, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf.

[11] Defendant's Motion to Dismiss, FTC v. Wyndham Worldwide Corp., No. 12-1365, at 11 (D. Ariz. Aug. 27, 2012) ("In the absence of any affirmative guidance as to what Section 5 requires in the world of data security, WHR cannot reasonably (or constitutionally) be found to have violated any of the FTC's post-hoc data-security standards.").

[12] Letter from Jennifer A. Hradil, Esq., to the Honorable Esther Salas, FTC v. Wyndham Worldwide Corp., No. 13-1887 (D.N.J. Feb. 6, 2014).

[13] FTC v. Wyndham Worldwide Corp., No. 13-1887 (D.N.J. Apr. 7, 2014) (denying defendant's motion to dismiss).

[14] FTC v. Wyndham Worldwide Corp., No. 13-1887, slip op. at 6–7 (D.N.J. Apr. 7, 2014).

[15] LabMD, Inc. v. FTC, No. 14-0810 (N.D. Ga. May 12, 2014).

[16] *See* Press Release, Fed. Trade Comm'n, Provider of Medical Transcript Services Settles FTC Charges that It Failed to Adequately Protect Consumers' Personal Information (Jan. 31, 2014) ("The FTC's consent order with GMR marks the 50th data security case the Commission has settled since undertaking its data security program 12 years ago."), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

[17] *See, e.g.*, MD. CODE ANN. COMM. LAW § 13-3503 (2013) ("To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.").

[18] CAL. CIV. CODE § 1798.81.5(b) (2013) ("A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.").

[19] MINN. STAT. § 325E.64 (2013).

[20] NEV. REV. STAT. § 603A.215(2) (2010).

[21] NEV. REV. STAT. § 603A.215(1) (2010).

[22] 201 MASS. CODE REGS. 17.00-17.05 (2009).

[23] Federal law does, however, impose notification requirements on certain entities maintaining medical information. *See* HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414 (requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information); *see also* 16 C.F.R. §§ 318.1–318.9 (FTC Health Breach Notification Rule). Additionally, an interpretative guidance issued by the Federal Financial Institutions Examination Council (FIFEC) in April 2005 sets forth general principles consistent with the majority of state data breach notification laws. The guidance was issued pursuant to section 501(b)(3) of the GLB Act, which authorizes agencies other than the CFPB to establish safeguards "to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

[24] Prepared Statement of the Fed. Trade Comm'n, Data Breach on the Rise: Protecting Personal Information from Harm, Senate Committee on Homeland Security and Governmental Affairs (Apr. 2, 2014) [hereinafter FTC Data Breach Statement], *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.

[25] Complaint, GMR Transcription Servs., Inc., FTC File No. 122 3095 (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140203gmrcmpt.pdf.

[26] Complaint, Accretive Health, Inc., FTC File No. 122 3077 (Dec. 31, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/131231accretivehealthcmpt.pdf.

[27] Complaint, Fandango, LLC, FTC File No. 132 3089 (Mar. 28, 2014); Complaint, Credit Karma, Inc., FTC File No. 132 3091 (Mar. 28, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140328fandangocmpt.pdf.

[28] *In re* Natural Provisions Inc., No. 522-9-13-WNCV (Vt. Super. Ct. Sept. 5, 2013).

[29] Tom Risen, *FTC Investigates Target Data Breach*, U.S. NEWS & WORLD REPORT (Mar. 26, 2014), *available at* http://www.usnews.com/news/articles/2014/03/26/ftc-investigates-target-data-breach.

[30] Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

[31] *See, e.g.*, Galria v. Nationwide Mut. Ins. Co., No. CV-118, 2014 WL 689703 (S.D. Ohio Feb. 10, 2014); Strautins v. Trustwave Holdings, Inc., No. 09115, 2014 WL 960816 (N.D. Ill. Mar. 12, 2014).

[32] S. 1976, 113th Cong. (2014).

[33] S. 1927, 113th Cong. (2014).

[34] S. 1995, 113th Cong. (2014).

[35] *See* FTC Data Breach Statement, *supra* note 24.

[36] Prepared Statement of the Federal Trade Commission, The FTC in FY 2013: Protecting Consumers and Competition, House Committee on Appropriations (Mar. 5, 2012) ("Consumer privacy remains at the top of the FTC's agenda."), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-ftc-fy-2013-protecting-consumers-and-competition/120305appropriationstestimony.pdf.