November 2015 A publication of the Data Breach, Cybersecurity and Privacy Team

The Arnold & Porter Data Security Roundup reports on recent legal developments in the realms of data security, data breach, data privacy, and cybersecurity. For more information on Arnold & Porter's related areas, please visit our Data Breach, Cybersecurity, and Privacy practices.

Executive and Regulatory Developments

FTC Loses Case Involving Security of Laboratory's Patient Data

On November 13, an administrative law judge for the FTC dismissed an August 2013 administrative complaint alleging that diagnostic laboratory LabMD had "failed to provide reasonable and appropriate security for personal information on its computer networks." The FTC's complaint stemmed from two incidents: one in which a spreadsheet of patient insurance information was found on a peer-to-peer file sharing network, and another where the Sacramento Police Department found LabMD documents, including names, Social Security numbers, and bank account information, in the possession of identity thieves. After over two years of proceedings, the FTC's administrative law judge found that LabMD's conduct did not constitute an unfair trade practice because the FTC failed to show that the "limited exposure of the [data at issue] has resulted, or is likely to result, in any identity theft-related harm." The judge also found that there was insufficient evidence to establish a causal connection between the alleged gaps in LabMD's security practices and the exposure of the data. Nor was there sufficient evidence to demonstrate that consumers were harmed or likely to be harmed by the "limited" exposure of data. The decision appeared to turn on strength and reliability of FTC's evidence. Of particular concern to the judge was the fact that the FTC relied on information from a company that had a financial incentive to find the alleged data breaches and sell remediation services. As a result, the decision may prompt the FTC to closely examine the cases it chooses to pursue in the future.

Senate Passes Cybersecurity Information Sharing Bill

On October 27, 2015, the Senate passed the Cyber Information Sharing Act (CISA), which will now go to conference with the House, which passed two similar bills earlier this year. All three bills function generally in the same way in that they permit companies to "monitor" their networks; permit sharing of "Cyber Threat Indicators" with the federal government; and permit private entities to deploy "defensive measures" to protect their systems. Finally, all three bills provide private entities immunity from most civil lawsuits related to monitoring information systems and reporting cyber threat indicators if such activities are done in accordance with the monitoring and sharing provisions of the respective bills, although all three bills do permit lawsuits to proceed against companies for "willful misconduct." CISA also permits lawsuits to proceed against companies for gross negligence, which does not require quite the showing of intentionality or recklessness that "willful misconduct" does. Though the aim of the bills is to facilitate sharing between private industry and the government, to accelerate responses -- and defenses -- to cyber threats, critics raise a host of concerns, including the broad definitions of information that may be shared, and the ability for the government to share information gathered with law enforcement for a number of broad purposes, including the threat of "economic harm." The conference process, and any future floor debates, may result in significant changes and amendments to any final bill, but given the overwhelming support for the measures in both houses of Congress, the eventual passage of some form of cyber sharing bill seems likely.

White House Decides Against Seeking Legislation to Require Companies to Provide "Back Doors" to Encrypted Data

On October 10, 2015, in a closely watched debate between Silicon Valley and the law enforcement and intelligence communities, the Obama Administration sided with industry and announced that it would not seek legislation that would provide the government with access to encrypted data contained on iPhones and other devices. Cryptographers and privacy advocates had argued that there is no way to create a "back door" to the encrypted data without rendering the data vulnerable to foreign intelligence agencies and cybercriminal and terrorist groups. In addition, Apple and other companies were concerned that the passage of such legislation might embolden foreign governments to pass similar or more invasive laws. Law enforcement has argued that encryption will make their jobs more difficult; however, in 2014, encryption was encountered in only a small fraction of wiretaps, and officials decrypted all but four of the 25 wiretaps that involved encryption.

Aftermath of the Court of Justice of the European Union Decision Invalidating the US-EU Data Protection Safe Harbor Framework

Since October 6, 2015, when the Court of Justice of the European Union (CJEU) issued a decision invalidating the US-EU Data Protection Safe Harbor Framework as it is currently formulated, there has been deep concern about the continued viability of transfers of personal data from the European Union to the United States. The CJEU decision (see *Batten Down The Hatches: The US-EU Data Protection Safe Harbor Framework Invalidated* (Oct. 7, 2015), available here) casts doubt on the authority of the EU Commission, which officially approved the Safe Harbor Framework in 2000, to determine on a pan-EU basis whether such a framework affords the level of data protection required by the European Parliament's directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

On November 6, a month after the CJEU issued its decision, the EU Commission issued guidance on permissible means to transfer personal data from the EU to the United States. In its guidance, the EU Commission provides several alternatives to the Safe Harbor Framework as a legal basis for trans-Atlantic data transfers, such as model contractual clauses and binding corporate rules (BCRs) (while questioning the viability of these options in light of the Working Party's concerns over US government surveillance). For further information and analysis, see Arnold & Porter's most recent client advisory on this issue here.

Litigation Developments

Update on *Spokeo*: Oral Argument

On November 2, the Supreme Court heard argument in *Spokeo, Inc. v. Robins*, No. 13-1339, a case concerning who has standing to bring lawsuits under the Fair Credit Reporting Act (FCRA). The Court is reviewing a Ninth Circuit ruling that Congress can confer standing to sue on consumers who have not been concretely injured and therefore would have otherwise lacked standing under the Constitution. The Court's decision could have significant implications for data breach suits, which often involve plaintiffs who allege violations of state or federal law but cannot show that a data breach caused them concrete injury. Several Justices expressed skepticism at the notion that a statutory injury is sufficient. If the Court reverses the Ninth Circuit and holds that a plaintiff must show more than statutory injury, the Justices will need to confront the separate question of whether the particular injury alleged by the plaintiff in *Spokeo* -- the dissemination of false information on the Internet -- is sufficiently concrete for constitutional purposes.

Target Court Rules Results of Data Breach Investigation Privileged

On October 23, 2015, the United States District Court for the District of Minnesota upheld Target's attempt to withhold as privileged certain materials related to a "Data Breach Task Force" that Target established to investigate its 2013 data breach, as well as certain documents created by Verizon, which was also retained by Target to investigate the breach. In upholding Target's claim of privilege, the court relied on the fact that the Data Breach Task Force was retained "so that the task force could educate Target's attorneys about aspects of the breach and counsel could provide Target with informed legal advice." With respect to Verizon, the Court was persuaded by the fact that Target had set up a two-track investigation to distinguish between investigatory work done in the ordinary course and investigatory work done at the direction of and for the purpose of assisting counsel. Specifically, on one track, Verizon conducted a non-privileged investigation on behalf of credit card companies so that Target and Verizon could learn how the breach happened and Target and the credit cards brands could respond appropriately. On the other track, a separate team from Verizon was engaged to educate Target's lawyers about the breach so they could provide Target with legal advice and

protect Target's interests in litigation that commenced almost immediately after the breach became public. The court determined that the latter type of work was entitled to be protected from disclosure. The ruling highlights the importance of ensuring that investigators hired in the wake of a data breach are retained and directed by counsel and that investigatory teams are appropriately structured with the protection of privilege in mind.

State Developments

California Signals Continued Focus on Data Privacy with Third Amendment to Data Breach Notification Laws in Three Years

California recently passed a trio of bills amending its data breach notification laws to bolster existing requirements for businesses affected by data breach. Among the changes enacted in this legislative package, signed by Governor Jerry Brown on October 6, 2015, is an expanded definition for "personal information" that now includes data captured by automated license plate recognition systems. In addition, California has set a new standard for data encryption, which now requires that encrypted data be "rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security." Finally, the amended law imposes new requirements for the specific language that must be used in security breach notifications and offers a model form that businesses may use as a template. The notices themselves must now be titled "Notice of Data Breach," and information about the data breach must be presented under predetermined headings that include "What Happened," "What Information Was Involved," "What We Are Doing," and "What You Can Do." The full text of the amended laws, which become effective on January 1, 2016, is available here (S.B. 34), here (A.B. 964), and here (S.B. 570).

New York State Department of Financial Services Recommends Regulations to Strengthen Cybersecurity Standards for Financial Institutions

In a letter to federal and state financial institution regulators dated November 9, 2015, the New York State Department of Financial Services (NYDFS) put forth a proposal for new cybersecurity regulations for financial institutions. The proposal is the result of a two-year investigation by the NYDFS into the current cybersecurity programs and practices of hundreds of banking organizations and insurers (the reports of those investigations are available here, here, and here). Among other data protection methodologies, the proposal would require multi-factor authentication for access to any internal data systems from an external network and new audit procedures. It would also set minimum standards for ensuring the security of sensitive data held by third-party service providers and require notification of "any cyber security incident that has a reasonable likelihood of materially affecting the normal operation of the entity." Further, the proposal would require each covered entity to maintain and implement written cybersecurity policies and procedures and to appoint a Chief Information Security Officer -- among other cybersecurity personnel -- to manage the entity's cybersecurity program. The NYDFS is soliciting feedback from eighteen state and federal regulatory organizations and hopes to use that input to develop comprehensive regulations in the coming months. The full text of the letter is available here.

Marcus A. Asner

Kenneth L. Chernof

Ronald D. Lee

Sharon D. Mayo

Angel Tang Nakamura

Nancy L. Perkins

Allyson Himelfarb

Julie A. Kent

Brad P. Abel

Tom McSorley

Brussels | Denver | Houston | London | Los Angeles

New York | San Francisco | Silicon Valley | Washington DC

arnoldporter.com