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

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

IN-HOUSE COUNSEL TIP

As part of the data security breach response plan you should have in place in the event of a security incident, create and maintain an up-to-date list of names and phone numbers of individuals who should be contacted, internally and externally, either to take action or for reporting purposes.

White House Issues Executive Order Authorizing Economic Sanctions Against Overseas Sources of Cyberattacks

On April 1, the White House issued an Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. The order authorizes economic sanctions against overseas individuals and entities that engage in significant, malicious cyber-enabled activities against U.S. interests and can be found here .

Senate Intelligence Committee Approves Cybersecurity Bill

On March 12, 2015, the Senate Select Committee on Intelligence approved the proposed Cybersecurity Information Sharing Act of 2015 (S. 754), in a nearly unanimous vote. The proposed legislation authorizes private entities to monitor their own information systems and operate defensive measures for cybersecurity purposes. It also encourages government and private entities to share information about cyber threat indicators and defensive measures. The bill shields private entities from liability for monitoring their own information systems and for sharing information about cyber threat indicators and defensive measures with the government, assuming they are in compliance with security standards. The bill further aims to increase privacy protections by, among other things, defining a limited scope of information permissibly shared, restricting the methods by which information is shared, and requiring private entities to take proactive steps to remove any personally-identifying information not directly related to the cyber threat prior to sharing. For further information and analysis, see Arnold & Porter Client Advisory Senate Intelligence Committee's Recent Cybersecurity Bill Doesn't Silence Privacy Advocates' Concerns, Despite A Dozen Amendments (March 27, 2015).

Three Data Security Breach Cases Dismissed

In March, three putative class actions stemming from data security breaches were dismissed, either due to lack of standing or to plaintiffs' inability to state a valid claim. In the first, filed

against national payroll service Paytime, Inc. in the wake of an unauthorized access to the company's computer networks, the court dismissed the case for lack of standing, finding that plaintiffs had alleged no actual misuse of the personal information that was accessed. *See Storm v. Paytime, Inc.*, No. 14-CV-1138, 2015 WL 1119724 (M.D. Pa. Mar. 13, 2015). In the second, filed in the Western District of Washington against national restaurant chain P.F. Chang's, the court concluded that the plaintiff had not stated plausible claims for relief, holding among other things that the restaurant chain did not contract with the plaintiff to provide a specific level of security and that therefore the plaintiff could not advance a breach of implied contract claim. The court also held that compliance with certain cybersecurity standards is unlikely to be material to plaintiff's decision about whether to shop or dine with a particular retailer, and thus the plaintiff lacked a basis for a claim for deceptive practices. *See Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL (W.D. Wash. Mar. 27, 2015). In the third case, the federal District Court for the District of New Jersey dismissed a putative class action against Horizon Blue Cross Blue Shield of New Jersey stemming from the theft of two password-protected laptops, holding the plaintiffs lacked standing because they could not show they had sustained any actual injuries that could be connected to the laptop theft. *See In re Horizon Healthcare Services, Inc. Data Breach Litigation*, No. 13-7418 (CCC) (D.N.J. March 31, 2015).[1] These cases demonstrate the difficulties plaintiffs continue to face in asserting claims based on data security breaches in the absence of actual misuse of their data.

[1]For disclosure purposes, we note that Arnold & Porter LLP represents Horizon Healthcare Services in this litigation.

Supreme Court Expected to Decide Soon Whether to Grant Certiorari in Spokeo

The Supreme Court is anticipated to decide soon whether to grant certiorari in *Spokeo, Inc. v. Robins*, No. 13-1339, a case with significant implications for standing in data security breach lawsuits. In *Spokeo*, the plaintiff alleges on behalf of a putative class that Spokeo, which operates a "people search" engine that aggregates publicly available information about individuals, published inaccurate information about him and others on the Internet in violation of the federal Fair Credit Reporting Act. The Ninth Circuit held that this bare statutory violation established constitutional standing to sue, even if the plaintiff suffered no harm to employment prospects or other tangible injury. If the Supreme Court takes the case and reverses, its decision could preclude plaintiffs from suing under state consumer protection laws based on alleged data security breaches, absent proof that their information has been misused, rather than simply exposed. A decision affirming the Ninth Circuit, by contrast, could pave the way for more class actions based on breaches. A ruling by the Court on the merits would only affect suits brought in federal court, however; state courts may establish their own standing rules. The Court is scheduled to consider the *Spokeo* petition at its April 17 conference and could announce its decision publicly as early as April 20. If the Court grants certiorari, it likely will hear argument in the case during the fall of 2015.

State Roundup

Montana and **Wyoming** amended their data security breach notifications laws to redefine what constitutes personally identifiable information, altering the types of data that would trigger a notification requirement. Notably, both states now include health and medical record information within the category of personally identifiable information. In addition, Wyoming has removed certain employment data from the definition, including a person's place of employment and employee identification number, and added other types of data, such as login and password information that would permit access to an online account. A separate bill amended Wyoming's law to require companies to provide "clear and conspicuous notice" to individuals affected by a data security breach, including at a minimum a general description of the breach, the approximate date of the breach, actions taken to guard against future breaches, and advice for how to remain vigilant in protecting against identity theft. Lastly,

Montana's law now requires companies to notify the state attorney general's Consumer Protection Office in addition to affected individuals, and insurance entities must also notify the state's insurance commissioner. The full text of Montana's law as amended, which becomes effective in October 2015, is available here . The amended provisions of Wyoming's law go into effect in July 2015 and are available here and here .

Connecticut created a new permanent department within the Office of the Attorney General this month titled the Privacy and Data Security Department. Formed to continue the work of an interdisciplinary Privacy Task Force appointed in 2011, the new department will work exclusively on investigations and litigation related to data security and consumer privacy. The announcement from Attorney General George Jepsen is available here .

To receive future editions of the Arnold & Porter Data Security Roundup, please click here.

For further information about Arnold & Porter's Data Breach, Privacy and Cybersecurity practices, please contact one of the Data Security team members here.

Your Data Security Roundup Editors:

Marcus A. Asner

Kenneth L. Chernof

Ronald D. Lee

Sharon D. Mayo

Angel Tang Nakamura

Nancy L. Perkins

Emilia P.E. Morris

Allyson Himelfarb

Julie A. Kent

Elisabeth S. Theodore