The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 22, No. 5 May 2014

Forecasting Developments In Privacy And Data Security Laws – Trends In Healthcare Protections Provide Lessons For All Companies

Kevin D. Lyles
Katherine S. Ritchey

Jones Day

According to the Privacy Rights Clearinghouse, 864,133,052 records containing sensitive personal information have been breached in 4,249 publicly reported incidents since 2005.[1] Recent high-profile data breaches hit a huge number of consumers and demonstrated the vulnerability and ubiquity of sensitive personal data. In light of the increased frequency and impact of data breaches, consumer protection advocates, government agencies, and legislatures are looking at data security requirements more closely to give data custodians and processors adequate incentives to proactively protect consumer data.

Congress has not yet enacted comprehensive data security legislation addressing data breaches, although there are several bills currently under consideration.[2] The calls for such legislation are getting louder and more insistent. Attorney General Eric Holder recently urged Congress to pass legislation requiring businesses to notify consumers and law enforcement of data breaches.[3] And the FTC remains a vocal proponent of federal data security legislation that strengthens the Commission's ability to impose data security standards on companies and requires companies to notify consumers of data breaches.[4]

Kevin D. Lyles

Katherine S. Ritchey

In the meantime, consumers whose information is compromised look for legal remedies. Historically, plaintiffs bringing claims against data custodians in response to data breaches have struggled to convince courts that they satisfy constitutional standing requirements and can quantify damages.[5] Plaintiffs advancing tort claims have tried to rely on the potential future harms that may result from unauthorized access to their personal information, but courts have generally found such claims insufficient to qualify as compensable damages without actual identity theft or use of the compromised information.[6] Moreover, plaintiffs in breach cases have found it difficult to show common harm sufficient for class treatment.[7]

Given all of these obstacles, data privacy statutes with statutory damages provide breach victims a clearer path to pursue a legal remedy for the unauthorized disclosure of their personal information.[8] But one significant problem for data breach victims using existing privacy statutes that provide for statutory damages is their narrow scope. The Telephone Consumer Protection Act was designed to protect consumers from unsolicited communications like faxes, robo-calls, and now text messages.[9] The Video Privacy Protection Act prohibits any "video tape service provider" from knowingly disclosing a customer's personally identifiable information.[10] The Electronic Communications Privacy Act, Wiretap Act and Stored Communication Act bar wiretapping and electronic eavesdropping,[11] and prohibit unauthorized access to stored communications.[12] The Fair and Accurate Credit Transactions Act prohibits a vendor from printing more than the last five digits of a credit or debit card number on a receipt. Each of these statutes certainly touches on issues of data privacy and protection, but even taken together they cover only a small portion of the field. As many would-be plaintiffs have discovered, consumers whose personal information is compromised by a corporate data breach can find it challenging to find a claim under one of these narrowly focused statutes.

Health information privacy is a heavily regulated and high-profile subject that has seen increased legislative attention in the last decade. It may not be surprising, then, that some consumer advocates argue that lawmakers should punish those companies that compromise financial and other information with the same types of tools used to enforce health information privacy under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").[13] Regardless of whether you believe such comprehensive legislation is realistic for general data breaches, in light of the effectiveness of HIPAA and the HITECH Act, forward-thinking companies can look to those laws as models and anticipate principles that could appear, at least in part, in a future general data breach statutory regime.

In general terms, HIPAA and the HITECH Act protect the privacy of elec-

Kevin D. Lyles *is a Partner in the Columbus office of Jones Day. He co-chairs the Outsourcing and Privacy & Data Security practices, with a focus on health care and life sciences transactions.* ***Katherine S. Ritchey*** *is a Partner in the San Francisco office of Jones Day and practices in the areas of complex commercial litigation, and privacy and data security. The authors thank* ***Soleil Tuebner, Colin Leary*** *and* ***Gabriel Ledeen*** *for their substantial contributions.*

Please email the authors at kdlyles@jonesday.com or ksritchey@jonesday.com with questions about this article.

tronically transmitted patient data, set forth data privacy and security standards, and establish notification requirements in the event of breaches of protected patient data. Violations of HIPAA and the HITECH Act carry civil and criminal penalties. The statutory history and implementation of HIPAA and the HITECH Act illustrate four trends with respect to the use of statutory penalties that may be instructive for entities trying to anticipate how statutory penalties may be used by regulators in the future outside of the healthcare industry:

• First, Congress has taken an increasingly broad view of who should be responsible for maintaining the privacy of protected data. Initially, HIPAA applied its privacy and security obligations and statutory penalties to "covered entities,"[14] and only indirectly reached downstream "business associates"[15] by requiring covered entities to contractually obligate business associates to observe certain privacy standards. The HITECH Act applied certain HIPAA obligations (and the associated statutory penalties for their violation) directly to business associates.[16] The direct threat of statutory penalties to business associates has greatly increased the stakes for vendors and contractors that service the healthcare industry.

• Second, Congress has increased penalties for violations of data privacy. The HITECH Act increased the relatively modest statutory penalty structure in HIPAA by, among other things: (1) substantially increasing both the minimum and maximum civil monetary penalty amounts that may be assessed by the Department of Health and Human Services ("DHHS") in a given case (the minimum penalty increased from $100 to $50,000, and the maximum from $25,000 to $1.5 million), which makes it easy for even isolated incidents to result in large liabilities; (2) establishing four intent-based tiers of violations and four corresponding tiers of penalties, all intended to reflect increasing levels of culpability;[17] and (3) removing a previously effective prohibition on penalties under circumstances in which the violator did not know (and with the exercise of reasonable diligence would not have known) of the violation.[18]

• Third, Congress is using broader enforcement tools to increase compliance with data privacy rules. While HIPAA originally was enforced by the Office of Civil Rights ("OCR") within DHHS, the HITECH Act granted concurrent enforcement authority to state attorneys general to obtain damages on behalf of state residents and enjoin further HIPAA violations.[19] Additionally, although neither HIPAA nor the HITECH Act provides for a private right of action, some more aggressive state-level medical privacy laws do,[20] and proponents of a federal statutory damages regime argue that the credible threat of private litigation – particularly class actions – creates a meaningful incentive for companies to exercise greater care in protecting data and helping consumers respond to data breaches.

• Fourth, HIPAA enforcement activity has dramatically increased and expanded to include preemptive audits. Prior to the passage of the HITECH Act, DHHS and OCR generally issued few penalties and audited covered entities only in response to breaches or complaints. Following the passage of the HITECH Act, DHHS and OCR began using their authority to issue civil monetary penalties more aggressively, and OCR has indicated that it expects enforcement activity to continue even with respect to relatively "small" breaches (reports involving fewer than 500 individuals). Additionally, Section 13411 of the HITECH Act requires DHHS to provide for periodic compliance audits of covered entities and business associates, and DHHS has conducted pilot programs and pre-audit readiness surveys in anticipation of rolling out a comprehensive HIPAA audit program.

If the enhanced penalties, scope and enforcement under the HITECH Act are harbingers of future data security legislation, then proactive companies may want to strengthen their own data privacy and security efforts to adopt some of the best practices from the healthcare industry. These would include conducting a data security risk assessment, adopting written policies and procedures, implementing a security breach response plan, and training workforce members on the handling of sensitive personal data.

1. Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breach (last visited Apr. 14, 2014).

2. *See, e.g.*, Data Security and Breach Notification Act of 2014, S.1976 113th Cong. (2014); Personal Data Protection and Breach Accountability Act, S.1995 113th Cong. (2013); Data Security Act of 2014, S.1927 113th Cong. (2014); Personal Data Privacy and Security Act of 2014, S.1897 113th Cong. (2014).

3. *A Message from the Attorney General: Protecting Consumers from Cybercrime and Identity Theft*, (February 24, 2014), http://www.justice.gov/agwa.php?id=4.

4. *See Prepared Statement of the Federal Trade Commission, "Protecting Consumer Information: Can Data Breaches Be Prevented?," Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce*, 113th Cong. 10 & n.35, Feb. 5, 2014, (statement of Edith Ramirez, chairwoman, Fed. Trade Comm'n), http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf

5. Patricia Cave, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits,* 62 Cath. U.L. Rev. 765 (2013).

6. *Id.* at 777-79.

7. *See, e.g., In re Hannaford Brothers Company Data Security Breach Litigation*, 293 F.R.D. 21 (D. Me. 2013).

8. *See Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014) (plaintiff's allegations of violations of his statutory rights under the Fair Credit Reporting Act satisfied Article III's requirement of an injury in fact because "the interests protected by the statutory rights at issue are sufficiently concrete and particularized that Congress can elevate them" to the status of legally cognizable injuries); *Charvat v. Mut. First Fed. Credit Union*, 725 F.3d 819 (8th Cir. 2013) (same); *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 953 (7th Cir. 2006) ("Yet individual losses, if any, are likely to be small – a modest concern about privacy, a slight chance that information would leak out and lead to identity theft. That actual loss is small and hard to quantify is why statutes such as the Fair Credit Reporting Act provide for modest damages without proof of injury."); *Harris v. comScore, Inc.*, 292 F.R.D. 579, 589 (N.D. Ill. 2013) (rejecting defendant's contention that the issue of individual loss or damage precluded class certification, noting that "[t]hat argument has no applicability to the ECPA or SCA claims, both of which provide for statutory damages), *aff'd comScore, Inc. v. Dunstan*, No. 13-cv-8007 (7th Cir. Jun. 11, 2013).

9. 47 U.S.C. § 227.

10. 18 U.S.C. § 2710(c)(2)(a).

11. 18 U.S.C. §§ 2511 et seq.

12. 18 U.S.C. §§ 2701 et seq.

13. *See, e.g.,* Laura Mahoney, *Witnesses Tell California Lawmakers State Needs Stiffer Breach Penalties*, Bloomberg BNA Privacy Law Watch, February 19, 2014, *available at* http://www.bna.com/witnesses-tell-california-n17179882357/.

14. HIPAA defines "covered entity" as health plans, health care clearinghouses and health care providers who transmit certain health information in electronic form. 45 C.F.R. § 160.103.

15. HIPAA defines a "business associate" generally to include persons who perform certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provide services to, a covered entity. *See* 45 C.F.R. § 160.103.

16. *See* 42 U.S.C. § 17931(a).

17. DHHS indicated in guidance that, generally speaking, it would measure the number of privacy violations (such as data breaches) by the number of individuals affected, and it would count continuing violations (such as failure to have appropriate safeguards in place) on a per-day basis. 78 Federal Register 5566, 5583-84 (January 25, 2013).

18. 42 U.S.C. § 1320d–5(a).

19. 42 U.S.C. § 1320d–5(d).

20. *See, e.g.*, Cal. Civ. Code § 56.101 (Deering 2014) (private right of action in California's Confidentiality of Medical Information Act).