Legal Backgrounder

Vol. 30 No. 10 May 8, 2015

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

A National Data-Breach Notification Standard: Why Federal Preemption Is Imperative

by Daniel I. Prywes and John C. Bush

One of the toughest challenges that consumer-facing businesses confront today is the secure maintenance of data. Consumers can suffer financial loss and inconvenience when their personal information is used in an unauthorized fashion following a data breach. Data breaches can also rob retailers and other businesses of consumer confidence and impose a variety of mitigation costs, such as consumer notification. For example, in 2013, Target suffered a steep loss of sales, and substantial remedial and litigation costs, after hackers stole credit, debit-card, and other personal information of approximately 110 million consumers.[1]

No federal law regulates the data-breach notification obligations of most industries, though several federal laws touch on this area. Congress is currently considering whether to enact a federal standard that would (a) establish a comprehensive federal obligation to protect consumers following data breaches; (b) preempt state data-breach statutes; and (c) preempt state common-law claims alleging deficient data-breach notification based on negligence or other theories of liability.

Federal Preemption Basics

The U.S. Constitution vests Congress with the power to "regulate Commerce . . . among the several States"[2] and make laws that shall be "necessary and proper" for carrying forth its powers.[3] The U.S. Supreme Court has explained that state laws that conflict with federal laws are "without effect,"[4] and "any state law, however clearly within a State's acknowledged power, which interferes with or is contrary to federal law, must yield."[5] When regulating interstate commerce, Congress has the authority to "occupy the field" and completely preempt all state laws on the same subject as the federal legislation.[6] Congress may also enact federal laws that permit the states to add stricter or supplemental requirements that do not directly conflict with a federal requirement.

---

[1] *See In Re Target Corp. Consumer Data Security Breach Litigation*, MDL No. 14-2522, 2014 U.S. Dist. LEXIS 175768, 2014 WL 7192478 (D. Minn. Dec. 18, 2014); Michael Riley, et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek, Mar. 13, 2014, *available at* http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

[2] U.S. Const., Art. I, Sec. 8, cl. 3.

[3] U.S. Const., Art. I, Sec. 8, cl. 18.

[4] *Maryland v. Louisiana*, 451 U.S. 725, 746 (1981).

[5] *Mutual Pharmaceutical Co. v. Bartlett*, 133 S. Ct. 2466, 2473 (U.S. 2013), quoting *Gade v. National Solid Wastes Mgt. Assn.*, 505 U.S. 88, 108 (1992).

[6] *Altria Group, Inc. v. Good*, 555 U.S. 70, 76 (2008); *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 372 (2000) ("When Congress intends federal law to 'occupy the field,' state law in that area is preempted").

Daniel I. Prywes is a partner with the law firm of Bryan Cave LLP, in Washington, D.C., and **John C. Bush** is an associate with Bryan Cave LLP in its Atlanta office. Both are members of the law firm's Data Privacy and Security Group.

Even where Congress does not "occupy a field" entirely, Congress has often exercised its preemption powers to prevent the states from imposing a patchwork of inconsistent or varying laws or standards that raise costs to businesses, burden interstate commerce, and interfere with the achievement of congressional objectives. For example, in the consumer area, Congress has preempted state laws dealing with electronic mail used to send commercial messages,[7] airline fares,[8] employee benefit plans,[9] and child online privacy protection.[10] Courts may also find that Congress has impliedly preempted state law where state laws stand "as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," or where "compliance with both federal and state regulations is impossible."[11]

Patchwork of State Data-Breach Laws

Currently, 47 states, plus the District of Columbia, U.S. Virgin Islands, Guam, and Puerto Rico have data-breach notification laws.[12] Those laws differ in many respects, such as in:

- the types of "personal information" that may trigger notification and reporting obligations after they are disclosed in a data breach;[13]
- whether the state's law includes exceptions to the customer-notification requirement where the custodian of information assesses that the risk of identity theft is low or that the breach has not materially compromised personal information;
- whether an individual state's data-breach notification law applies to entities that do not do business in the state but maintain personal information about state residents;
- whether the state law's customer-notification requirements are triggered when customer information is accessed but not acquired through the breach;
- whether the state's law requires that notice of a breach must be given only to state residents or, in some circumstances, to affected persons anywhere;
- the scope of information that must be included in notifications to customers, and the method of communication and deadlines by which notification must be provided;
- the data-breach notification duties of firms that maintain customers' personal information on behalf of other firms;

[7] 15 U.S.C. § 7707(b) (CAN-SPAM law preempts any state law that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute . . . prohibits falsity or deception in any portion of a commercial electronic mail message").

[8] 49 U.S.C. § 41713(b) (Federal Aviation Administration Authorization Act of 1994 preempts non-federal laws "related to a price, route, or service of an air carrier that may provide air transportation").

[9] 29 U.S.C. § 1144 (ERISA "shall supersede any and all State laws insofar as they may now or hereafter relate to any employee benefit plan" covered by ERISA, subject to exceptions). *See Aetna Health Inc. v. Davila*, 542 U.S. 200, 209 (2004).

[10] 15 U.S.C. § 6502(d) (the Children's Online Privacy Protection Act preempts "inconsistent" state laws concerning the online collection of personal information from children).

[11] *Hillman v. Maretta*, 133 S. Ct. 1943, 1950 (2013) (citations omitted).

[12] *See* Valdetero and Zetoony, *Data Security Breaches: Incident Preparedness and Response*, at 31-38, Washington Legal Foundation Monograph (2014), *available at* http://wlf.org/upload/legalstudies/monograph/ValdeteroZetoonyFinal.pdf.

[13] *E.g., compare* O.C.G.A. § 10-1-911(6) (Georgia defines "personal information" as the use of a name in combination with other data points when at least one is unencrypted), *with* C.G.S.A. § 36a-701b(a) (Connecticut defines "personal information" without reference to its encryption).

- whether and in what circumstances state regulatory agencies and credit reporting agencies must be informed of data breaches and the scope of penalties; and

- whether consumers have a private right of action to enforce violations of state-law requirements.

Consumer and Marketplace Benefits of Federal Preemption

The current situation—a patchwork of state laws and a problem of national and international scale—presents a classic example of why Congress' constitutional authority to preempt inconsistent or varying state laws is so vital. A federal data-breach standard cannot protect consumers or achieve regulatory uniformity in a national market without preemption of state statutes and state common-law claims regulating the scope and timing of required data-breach notifications. Under such an approach, Congress could allow states to continue to police fraudulent or deceptive conduct, much as in other areas where states are permitted to combat fraud alongside an otherwise preemptive federal framework.

When a data breach occurs in the current state-by-state regulatory environment, the data-holding firm must wade through the morass of dozens of jurisdictions' laws to determine its duties and the required response because the effects of a data breach are rarely limited to consumers in a single state. For example, most states' laws only require that organizations give notice of data breaches to consumers located in their particular state, but several states (including Hawaii, New Hampshire, North Carolina, and Texas)[14] require that any organization conducting business in the state also give notice to affected consumers located in any state, including those in the three states (Alabama, New Mexico, and South Dakota)[15] which have no data-breach notification laws of their own. Some states have unique requirements as to the notices themselves, such as Massachusetts which prohibits an organization from identifying in a consumer notification the nature of the data breach or the number of Massachusetts residents affected by the breach.[16]

The substantial regulatory burden of compliance with so many divergent data-breach notification laws falls on large and small businesses alike, creating costs that the businesses ultimately pass on to consumers. With a single federal law, businesses could more easily and efficiently determine their rights and responsibilities. Without preemption, a new federal law would simply add an additional statute on top of the many existing state laws, thus adding to the regulatory burden rather than reducing it.

The welter of state laws also provides uneven protection for consumers. A uniform federal standard would benefit consumers by enabling them to: (a) determine easily their rights; (b) avoid complex legal disputes that can arise in identifying the controlling state's law; (c) eliminate variations among the states as to whether the economic loss doctrine bars consumer claims; and (d) enable the federal government to apply its enormous resources and enforcement power with respect to retailers and other firms that do business nationally. The complexity in current enforcement efforts is illustrated by the trial court's December 18, 2014 ruling in the Target data-breach litigation. The court sorted through numerous states' data-breach and consumer protection laws, and determined that class members in different states had different rights under those laws with respect to the same data breach.[17] For example, the court ruled that no class actions could

[14] Haw. Rev. Stat. § 487N-2(a); N.H. Rev. Stat. Ann. § 359-C:20(I)(a); N.C. Gen. Stat. Ann. § 75-65(a); Tex. Bus. & Com. Code Ann. § 521.053(b).

[15] *See* Valdetero and Zetoony, *Data Security Breaches*, *supra* note 12.

[16] Mass. Gen. Laws Ann. ch. 93H, § 3.

[17] *In Target Corp. Consumer Data Security Breach Litigation*, *supra*, at *15-38; *see also* McKenna and Lindlaw, *Targeting Harm from a Data Breach: Federal Judge Lets Plaintiffs Get Away with Kitchen-Sink Pleading*, Washington Legal Foundation LEGAL BACKGROUNDER, Mar. 27, 2015, available at http://www.wlf.org/upload/legalstudies/legalbackgrounder/032715LB_McKenna1.pdf.

ISBN 1056 3059

be brought in federal court for violation of eight states' consumer protection laws which prohibited class actions; no private action was allowed under 12 states' data-breach notification laws; and that the economic loss rule barred negligence claims in five states.[18]

In addition, to address the multiple state laws now on the books, some firms currently choose to adhere to the strictest states' laws, even if these states are costly outliers that impose burdens that most states have rejected. By preempting such state laws, Congress could avoid this undesirable scenario in which one or more states can, in practice, burden commerce on a national scale. Congress can ensure that federal standards strike an appropriate balance between consumer protection and running a business efficiently.

By preempting state law, Congress could determine on a national basis when businesses must notify and protect consumers from a data breach, and when a breach poses such little risk that notification is not warranted. It is well recognized that "over-notification" (*i.e.*, notification where there is no significant risk of injury) can numb consumers to data-breach notifications so that they do not take necessary action when a more serious breach occurs.[19] The existing situation can cause widespread confusion as consumers in a state which does not require notification of low-risk breaches hear about data-breach notifications in other states that do require notification of virtually all data breaches.

Finally, state common-law claims alleging a failure to provide adequate data-breach notification should also be preempted because they are likely to undermine federal standards otherwise. Individual juries applying different states' laws could differ on whether steps taken to notify consumers of data breaches were "reasonable" or "negligent," and different standards of "reasonableness" could be developed by different states' courts. Without federal preemption in this area, retailers and other firms would have no reliable polestar to determine how to proceed in responding to data breaches.

As the Supreme Court has recognized, the purpose of a federal statute "can be undermined just as surely by a state common-law rule as it can by a state statute or regulation."[20] By preempting state common-law claims for data-breach notification, Congress could ensure a uniform federal standard—the key advantage of federal preemption for consumers and businesses alike.

In sum, by preempting state laws and claims, Congress can promote a more efficient and uniform system for addressing data breaches and make it easier for consumers to determine their rights.

---

[18] *In Target Corp. Consumer Data Security Breach Litigation*, *supra* note 1 at *24, 37-38, 52.

[19] *E.g.*, Sarah Halzack, *Home Depot and JPMorgan are doing fine. Is it a sign we're numb to data breaches?* WASH. POST., Oct. 6, 2014, *available at* http://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/.

[20] *Northwest, Inc. v. Ginsberg*, 134 S. Ct. 1422, 1430 (2014) (Airline Deregulation Act preempts state common-law claims for a state-imposed implied covenant of good faith and fair dealing in contracts).

  ISBN 1056 3059