Data Security and Breach Notification Legislation: Selected Legal Issues

Alissa M. Dolan
Legislative Attorney

December 28, 2015

Congressional Research Service
7-5700
www.crs.gov
R44326

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Recent data breaches at major U.S. retailers have placed a spotlight on concerns about the security of personal information stored in electronic form by corporations and other private entities. A data breach occurs when data containing sensitive personal information is lost, stolen, or accessed in an unauthorized manner, thereby causing a potential compromise of the confidentiality of the data. Existing federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the Gramm-Leach-Bliley Act, impose security and breach notification requirements on specific industries or types of data. Additionally, 47 states, the District of Columbia (D.C.), and three territories have enacted laws requiring breach notification, while at least 12 states have enacted data security laws, designed to reduce the likelihood of a data breach. Alabama, New Mexico, and South Dakota have not enacted breach notification laws.

Several data security and breach notification bills have been introduced in the 114th Congress, which broadly would impose security and notification requirements on businesses regardless of industry sector, with limited exceptions. This report begins by describing the common elements of these federal proposals and then discusses state laws that may apply in the event of a data breach.

The report then addresses two legal issues that may arise in consideration of new legislation about data security and breach notification. First, how would new federal legislation alter the application of existing state law or the availability of state law remedies for victims of data breaches? The report will discuss various forms of federal preemption (including express preemption, implied impossibility preemption, and implied obstacle preemption) and evaluate how a reviewing court might apply these preemption principles to federal proposals to determine which state laws would be superseded.

Second, the report examines the existing jurisdiction and enforcement authority of the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) with regard to data security and breach notification requirements. This section analyzes the FTC's unfair or deceptive acts and practices authority under the Federal Trade Commission Act and the FCC's authority to regulate data security and breach notification for common carriers and cable and satellite providers under the Communications Act. Finally, it evaluates how the current federal proposals would change the enforcement responsibilities of each agency, potentially increasing the jurisdiction of the FTC and limiting the FCC's ability to enforce its existing data security rules.

Contents

Contacts

Introduction

Recent data breaches at major U.S. retailers have placed a spotlight on concerns about the security of personal information stored in electronic form by corporations and other private entities. A data breach occurs when data containing sensitive personal information is lost, stolen, or accessed in an unauthorized manner, thereby causing a potential compromise of the confidentiality of the data. Existing federal law imposes security and breach notification requirements on specific industries or types of data. For example, certain health information is subject to requirements under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), while certain financial institutions are subject to requirements under the Gramm-Leach-Bliley Act (GLB).[1] Additionally, 47 states, the District of Columbia (D.C.), and three territories have enacted laws requiring breach notification,[2] while at least 12 states have enacted data security laws.[3]

Several data security and breach notification bills have been introduced in the 114th Congress, which broadly would impose security and notification requirements on businesses regardless of industry sector, with limited exceptions. Many of the current proposals would leave existing federal requirements in place and exempt institutions and/or data covered by those federal laws from a new regulatory scheme. However, some bills would also propose to supersede existing state laws and prevent states from acting in this area, thereby creating a uniform federal standard throughout the country.

During consideration of proposed bills, two prominent legal issues have arisen. First, to what extent would federal legislation preempt state and local actions (including statutes, regulations, and/or the ability to bring legal claims) regarding data security and breach notification? Second, what effect would such legislation have on the existing authority of the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) to bring enforcement actions related to data security and breach notification?

This report will discuss these two issues, starting with an examination of the Supreme Court's precedent regarding federal preemption. It will then analyze how these preemption principles might be applied by a reviewing court seeking to determine the preemptive effect of different federal proposals. Next, it will examine the existing jurisdiction and enforcement authority of the FTC and the FCC with regard to data security and breach notification as applied to telecommunications providers and how these agencies' responsibilities might be altered by proposed legislation.

[1] The Federal Information Security Management Act (FISMA) establishes standards for security and breach notification for information stored by federal agencies. P.L. 107-347, Title II, as amended by P.L. 113-283, *codified at* 44 U.S.C. §§ 3551, et seq. This report does not discuss requirements and considerations related to federal agency data.

[2] For a list of all state and territory statute citations, *see* National Conference of State Legislatures, "Security Breach Notification Laws," http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. As of October 22, 2015, Alabama, New Mexico, and South Dakota do not have data breach notification laws.

[3] *See infra* note 17.

Proposed Legislation on Data Security and Breach Notification

Several bills relating to data security and breach notification have been introduced in the 114th Congress.[4] The bills take different approaches to imposing data security requirements on covered entities, if at all. For example, some bills establish specific criteria required for a covered entity's data security program, including elements such as design, risk assessment and management, and employee training.[5] Other bills empower the FTC to write rules regarding data security, and require the FTC to address certain topics in those rules.[6] Still others simply state that covered entities must employ reasonable security measures and practices, without identifying what those measures and practices must be.[7] In general, a violation of the data security requirements or standards would be considered to be an unfair or deceptive act or practice, enforceable by the FTC.

Regarding notification, generally, a covered entity is required to provide notice when personal information contained in electronic data that it owns or possesses is either (1) accessed *or* acquired or (2) accessed *and* acquired, without authorization. Each bill defines what entities are covered and what constitutes personal information. Notification must usually be provided to residents and/or citizens of the United States as well as to the FTC and, in some cases, credit reporting agencies. Each bill establishes a deadline for notification, either within a certain number of days (such as 30 or 45 days) or as "expediently as possible and without unreasonable delay" after discovering the breach. Delayed notification is required if notice would jeopardize certain kinds of law enforcement investigations or national security.

Each bill defines the required form of notification, which may include written notice by mail or notice by email, when certain conditions are met. In certain circumstances, substitute notification through a posting on a website or publication may be an acceptable replacement for individual notification. The content of the notification includes such elements as the kind of personal information that has been breached, a phone number to contact for further information, and, potentially, information about the availability of free credit reporting services. However, in most cases, if the covered entity determines that the breach poses no reasonable risk of identity theft, fraud, or other unlawful conduct, then notification is not required. Notification requirements may also be waived if the entity is already required to provide notice under an existing federal law, such as HIPAA or GLB.

Violations of the notice requirements would typically be classified as unfair or deceptive acts or practices, which would be enforced by the FTC under existing regulations. Some bills would specifically empower the FTC to write regulations to implement the notification requirements, while others would not.[8] Along with enforcement by the FTC, some of the proposals allow state

[4] This report will reference the following bills: H.R. 580, the Data Accountability and Trust Act; H.R. 1053 and S. 547, the Commercial Privacy Bill of Rights Act of 2015; H.R. 1704, the Personal Data Notification and Protection Act; H.R. 1770, the Data Security and Breach Notification Act of 2015; H.R. 2205 and S. 961, the Data Security Act of 2015; S. 177, the Data Security and Breach Notification Act of 2015; S. 1027, the Data Breach Notification and Punishing Cyber Criminals Act of 2015; and S. 1158, the Consumer Privacy Protection Act of 2015.

[5] *See, e.g.*, S. 1158, § 202.

[6] *See, e.g.*, H.R. 580, § 2(a).

[7] *See, e.g.*, H.R. 1770, § 2.

[8] *See, e.g.*, H.R. 580, § 3(i) (granting the FTC authority to promulgate regulations to "effectively enforce" the bill's notification requirements); H.R. 1770 (providing no specific grant of rulemaking authority to the FTC).

attorneys general to enforce violations of the rules that affect people in their state through the filing of civil actions.[9]

Some bills contain additional provisions that go beyond security and breach notification and address topics such as data privacy.[10] Additionally, as discussed further below, some bills specifically address the treatment of telecommunications common carriers, while others are silent on the subject. The details of each bill differ and close inspection of each provision and definition is required to determine its specific effect.

State Laws Pertaining to Data Security and Breach Notification

Forty-seven states, D.C., Guam, Puerto Rico, and the U.S. Virgin Islands have enacted legislation requiring businesses to notify affected persons when a data breach occurs.[11] For example, California law requires that businesses that own or license computerized data that include personal information provide notice of a data breach to residents of California in the "most expedient time possible and without unreasonable delay."[12] A breach occurs when such unencrypted data is "acquired by an unauthorized person."[13] The required notice may be delayed if a law enforcement agency determines that the notice "will impede a criminal investigation."[14] The notice must be written in plain language and provide specific information: the name and contact information of the reporting entity; the type of personal information involved in the breach; the approximate date of the breach, if known; a general description of the "breach incident"; and, in certain circumstances, information about credit reporting agencies and identity theft prevention.[15] In addition to notifying individuals whose information is acquired, if the breach affects more than 500 California residents, the entity must also notify the state attorney general.[16]

At least 12 states also have laws specifically addressing data security.[17] For example, Massachusetts has promulgated regulations requiring persons who own or license personal information about a Massachusetts resident to "develop, implement, and maintain a

[9] *See, e.g.*, H.R. 1704, § 108; S. 177, § 5(d).

[10] *See, e.g.*, H.R. 1053.

[11] For a list of all state and territory statute citations, *see* National Conference of State Legislatures, "Security Breach Notification Laws," http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. As of October 22, 2015, Alabama, New Mexico, and South Dakota do not have data breach notification laws.

[12] CAL. CIV. CODE § 1798.82(a).

[13] *Id*.

[14] *Id*. at § 1798.82(c).

[15] *Id*. at § 1798.82(d).

[16] *Id*. at § 1798.82(f).

[17] Arkansas (ARK. CODE § 4-110-104); California (CAL. CIV. CODE § 1798.81.5); Connecticut (Conn. Pub. Acts No. 08-167); Florida (FLA. STAT. §§ 282.318, 501.171); Indiana (IND. CODE § 24-4.9-3-3.5); Maryland (MD. CODE ANN., COM. LAW § 14-3501); Massachusetts (201 MASS. CODE REGS. § 17.00) (issued pursuant to MASS. GEN. LAWS ch. 93H); Nevada (NEV. REV. STAT. § 603A.210); Oregon (OR. REV. STAT. § 646A.622); Rhode Island (R.I. GEN. LAWS § 11-49.2); Texas (TEX. BUS. & COM. CODE § 48.102); Utah (UTAH CODE § 13-44-201). Other state laws may impose data protection requirements on information held by the state government. For example, Montana recently enacted a law requiring state agencies that maintain personal information to develop procedures to protect that data. H.B. 123, § 26 (2015).

comprehensive information security program.... "[18] Such a program must be in writing and contain administrative, technical, and physical safeguards that are appropriate based on the size and type of business, available resources, and the amount of stored data.[19] Every program shall complete specific tasks, such as "identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity" of data; developing employee security policies on storage, access, and transportation of records; and regularly monitoring the program to ensure that it is "operating in a manner reasonably calculated to prevent unauthorized access" to data.[20] Businesses must also conduct an annual review of security measures.[21]

Finally, states may have general consumer protection laws that could potentially be used to remedy the harm caused by a data breach. For example, Illinois law makes unlawful "unfair methods of competition and unfair or deceptive acts or practices ... in the conduct of any trade or commerce."[22] This law includes prohibitions on "deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression, or omission of any material fact, with intent that others rely upon the concealment.... "[23] Individuals whose personal information is compromised in a data breach may attempt to use such a consumer protection law to allege that the breached entity's failure to disclose its inadequate security measures amounts to an unfair or deceptive practice in violation of state law.[24]

Preemption of State Laws, Regulations, and Claims

A major question related to consideration of federal legislation addressing data security and breach notification is whether, and to what extent, the federal law should preempt these existing state laws, thereby displacing state-by-state requirements in favor of a uniform, federal standard for entities covered under the general requirements established in the proposed legislation discussed above.

Federal preemption is rooted in the Supremacy Clause of the U.S. Constitution, which states that "[t]he Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land."[25] Under the Supremacy Clause, Congress can override any state and local law that falls within Congress's legislative authority.[26] Therefore, the legal issue is not whether Congress has the ability to preempt state and local laws but rather determining the

[18] 201 MASS. CODE REGS. 17.03(1).

[19] *Id*.

[20] *Id*. at 17.03(2).

[21] *Id*. at 17.03(2)(i).

[22] 815 ILL. COMP. STAT. 505/2.

[23] *Id*.

[24] It may be difficult for plaintiffs to prevail on claims brought under a state general consumer protection statute due to the specific elements that must be proven in order to succeed on such a claim. *See, e.g.*, In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518 (N.D. Ill. 2011) (concluding that the plaintiffs failed to allege a deceptive practice under the Illinois Consumer Fraud and Deceptive Business Practices Act because plaintiffs could not identify any communications by Michaels, the subject of the data breach, containing the allegedly deceptive omission—that it did not implement adequate security measures). Required elements may differ in each state's law.

[25] U.S. CONST. art. IV, cl. 2.

[26] Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 372 (2000) ("A fundamental principle of the Constitution is that Congress has the power to preempt state law.").

particular circumstances under which federal law, either explicitly or implicitly, preempts state and local laws.

In answering the question of when preemption occurs, the Supreme Court has at times emphasized "two cornerstones of [] pre-emption jurisprudence."[27] First, "the purpose of Congress is the ultimate touchstone in every pre-emption case."[28] Second, "[i]n all pre-emption cases, and particularly in those in which Congress has 'legislated ... in a field which the States have traditionally occupied,' we 'start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.'"[29] There are two kinds of federal preemption: express preemption and implied preemption.[30]

Express Preemption

Express preemption occurs when a federal statute explicitly states its intent to preempt state and/or local action on a given subject. By including such language, Congress expresses its clear intent that the federal statute is to supersede state attempts to regulate on the issue. If a federal law is deemed to preempt a state law, regulation, or cause of action, then the preempted state law, regulation, or cause of action cannot be the basis for enforcement against covered entities.

Congress may also choose to include a "saving clause" in addition to an express preemption clause. A saving clause seeks to preserve some role for state or local action, by "saving" certain actions from the scope of the express preemption clause. Where a saving clause is present, the express preemption clause and saving clause must be read together in order to determine what kinds of actions will ultimately be superseded under express preemption principles.[31]

All of the current federal legislative proposals in the area include express preemption clauses. Each express preemption clause typically raises at least two different issues: first, the *types* of

[27] Wyeth v. Levine, 555 U.S. 555, 565 (2009).

[28] Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996).

[29] *Id*. (quoting Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947)). Some commentators have noted that the presumption against preemption has not been uniformly applied in recent Supreme Court cases. *See, e.g.*, Ernest A. Young, *"The Ordinary Diet of the Law": The Presumption Against Preemption in the Roberts Court*, 2011 SUP. CT. REV. 253, 307 (2011) ("In theory, at least, the centerpiece of modern preemption doctrine remains the Court's statement in *Rice v. Santa Fe Elevator Corp.* that 'we start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.' Just three years ago, in *Wyeth*, the Court described the *Rice* presumption as a 'cornerstone[] of our pre-emption jurisprudence.' Notwithstanding this and similar endorsements, many scholars have noted the Court's failure to consistently employ the *Rice* canon. The 2010 Term was no exception to this tendency: The Justices ignored *Rice* in *Williamson* and *Concepcion* and invoked it only in dissent in *PLIVA* and *Bruesewitz*. In *Whiting*, the majority looked only to the 'plain wording' of the express preemption clause, but imposed a 'high threshold' for finding conflict preemption."); Thomas W. Merrill, *Symposium: Ordering State-Federal Relations Through Federal Preemption Doctrine: Preemption and Institutional Choice*, 102 NW. U.L. REV. 727, 741-43 (2008); Mary J. Davis, *Unmasking the Presumption in Favor of Preemption*, 53 S.C. L. REV. 967 (2002).

[30] Implied preemption can be further broken down into two categories, field preemption and conflict preemption, discussed below. *See* "Implied Conflict Preemption."

[31] Geier v. American Honda Motor Co., 529 U.S. 861, 868 (2000). In *Geier*, the Supreme Court held that the preemption and saving clauses of the National Traffic and Motor Vehicle Safety Act of 1966 had to be read together such that the text of both clauses is given "actual meaning." *Id*. *See also* Sprietsma v. Mercury Marine, 537 U.S. 51 (2002).

state and local actions[32] intended to be displaced and second, the *subject matter* of the preempted actions. For example, the express preemption clause in H.R. 1770 states:

> No State or political subdivision of a State shall, with respect to a covered entity subject to this Act, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a security breach of such data.[33]

The type of state and local actions covered by this clause would be "any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law.... "[34] The subject matter of the preempted actions would be those "relating to or with respect to the security of data in electronic form or notification following a security breach of such data."[35] Therefore, if a state action is of the type covered by the clause, falls within the subject matter of the clause, and is adopted, maintained, enforced, or imposed or continued in effect by the state, the action will be expressly preempted under this clause.

When evaluating express preemption clauses, courts rely on principles of statutory interpretation to determine if a given state or local action is preempted. In trying to effectuate congressional intent, courts look to the "language of the pre-emption statute and the 'statutory framework' surrounding it"[36] as well as the "'structure and purpose of the statute as a whole.'"[37] Therefore, analyzing an express preemption clause is a context-driven exercise, where the specific words in the statute and the intent of the legislative scheme as a whole are of crucial importance.

Types of Actions Being Preempted

Congress can choose to displace any state or local action in an express preemption clause. State actions subject to federal preemption could include positive law enactments, such as state statutes and regulations. State common law, such as the ability to bring lawsuits under theories including breach of contract, negligence, or other torts, can also be preempted by federal law. Both positive law enactments and state common law claims will be referred to as "state actions" throughout this report.

Positive Law

All of the express preemption clauses in the proposed federal data security and breach notification bills are likely to be interpreted as preempting state positive law enactments governing the specific subject matter. Express preemption clauses that use words such as "law," "statute," and/or "regulation" would preempt positive enactments of state and local law. Additionally, positive law enactments clearly impose "requirements" or "prohibitions"[38] and, therefore, clauses using those phrases will also have the effect of preempting state positive law.

---

[32] State and local actions could include the enactment of state statutes, promulgation of regulations, and the ability to bring legal claims under state common law.

[33] H.R. 1770, § 6(a).

[34] *Id*.

[35] *Id*.

[36] *Medtronic*, 518 U.S. at 486 (quoting Gade v. National Solid Wastes Management Ass'n, 505 U.S. 88, 111 (1992) (Kennedy, J., concurring in part and concurring in judgment)).

[37] *Id*. (quoting *Gade*, 505 U.S. at 98).

[38] *See* Cipollone v. Liggett Group, 505 U.S. 504, 521 (1992).

Common Law Causes of Action

Less clear is which of the proposed bills are likely to be interpreted as also preempting common law causes of action.[39] The Court has ruled that express preemption clauses referring to "requirements," "standards," or "other provisions with the force or effect of law" cover duties imposed by common law and, therefore, could preempt common law causes of action.[40] For example, in *Cipollone v. Liggett Group*, a plurality of the Supreme Court held that a provision preempting a state-imposed "requirement or prohibition based on smoking and health" "plainly reaches beyond [positive] enactments" and "easily encompass[es] obligations that take the form of common-law rules.... " since the common law actions at issue were premised on the existence of a legal duty.[41] Furthermore, the Court's precedent indicates that the word "rule" in the phrase "any provision of statute, rule, or regulation" arguably encompasses common law claims.[42] In *Sprietsma*, the Court noted that if one interpreted the word "law" in the phrase "law or regulation" (as used in the express preemption clause) to encompass both positive law enactments and common law rules, then the term "regulation" becomes superfluous.[43] Similarly, here, one could argue that if one interprets "statute, regulation, or rule" as encompassing only positive law enactments, then the use of the word "rule" is superfluous. Therefore, the better interpretation of the phrase, that gives meaning to each of the words contained therein, appears to be one that encompasses both positive law enactments and common law rules. Therefore, bills that use this wording likely would preempt common law causes of action.

Bills preempting "any provision of the law of any state" may also be interpreted to include common law claims within the scope of express preemption.[44] The Court has noted that "[i]t is routine to call common law rules 'provisions'"[45] and federal courts have previously treated

---

[39] *See, e.g.*, H.R. 580, § 6(a) ("This Act supersedes any provision of a statute, regulation, or rule of a State ... "); H.R. 1770, § 6(a) ("No State or political subdivision of a State shall, with respect to a covered entity subject to this Act, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law ... "); H.R. 2205, § 6 ("No requirement or prohibition may be imposed under the laws of any State ... "); S. 177, § 7(a) ("[T]his Act supersedes any provision of a statute, regulation, or rule of a State ... "); S. 961, § 6 ("No requirement or prohibition may be imposed under the laws of any State ... "); S. 1027, § 8 ("This Act preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State ... ").

[40] *Cipollone*, 505 U.S. at 521 (determining that the term "requirement or prohibition" encompasses common law obligations); *see also* Bates v. Dow Agrosciences, 544 U.S. 431, 443 (2005) (concluding that the term "requirement" in the express preemption clause of the Federal Insecticide, Fungicide, and Rodenticide Act "reaches beyond positive enactments, such as statutes and regulations, to embrace common-law duties"); Northwest, Inc. v. Ginsberg, 134 S. Ct. 1422 (2014) (declaring that state common law rules fall comfortably within a provision preempting a state "law, regulation, or other provision having the force and effect of law ... "); CSX Transp. v. Easterwood, 507 U.S. 658, 664 (1993) (finding that legal duties imposed by common law fall within the scope of a clause preempting any state "law, rule, regulation, order, or standard relating to railroad safety").

[41] *Cipollone*, 505 U.S. at 521.

[42] The Supreme Court frequently refers to common-law claims and obligations as "rules." *See, e.g.*, *Ginsberg*, 134 S. Ct. at 1429-30; Altria Group, Inc. v. Good, 555 U.S. 70, 81 (2008); *CSX Transp.*, 507 U.S. at 675; *Cipollone*, 505 U.S. at 521-22.

[43] *Sprietsma*, 537 U.S. at 63.

[44] *See, e.g.*, H.R. 1053, § 156 ("The provisions of this title shall supersede any provisions of the law of any State.... "); H.R. 1704, § 109 ("The provisions of this title shall supersede any provision of the law of any State.... "); S. 547, § 156 ("The provisions of this title shall supersede any provisions of the law of any State.... "); S. 1158, § 220 ("[T]he provisions of this subtitle shall supersede... any provisions of the law of any State.... ").

[45] *Ginsberg*, 134 S. Ct. at 1429 (citing Madsen v. Women's Health Center, Inc., 512 U.S. 753, 765 (1994); United States v. Barnett, 376 U.S. 681, 689-700 (1964); Brown v. United Airlines, Inc., 720 F.3d 60, 68 (1st Cir. 2013)). Additionally, the Supreme Court has suggested that the use of the term "law" alone in an express preemption clause (continued...)

common law claims as the type of claim that could be preempted in statutes that supersede "any provision of state law."[46] While this appears to be the best interpretation of this type of bill, the case law does not provide clear answers. It is likely that both the continued viability of the presumption against preemption[47] and the text and purpose of the broader statutory scheme would have to be closely considered before deciding the appropriate interpretation of these clauses.[48]

If common law actions are eligible for preemption under an express preemption clause, a reviewing court must still determine if the specific action being brought satisfies all elements of the clause. Not all common law actions may be considered to be laws of the state or laws imposed by the state. For example, on several occasions, the Supreme Court has drawn a distinction between common law claims that seek to enforce obligations imposed by the state and claims that derive from self-imposed obligations, voluntarily undertaken by the parties. In *American Airlines v. Wolens*, the Court concluded that although some common law claims could be preempted under the express preemption clause at issue, a breach of contract claim would not be superseded because the contract represented "privately ordered obligations," not provisions that were enacted or enforced by the state.[49] Therefore, a common law claim that seeks to enforce self-imposed

(...continued)

may lead to a different meaning than if the clause applied to both "law" and "regulation." *See Sprietsma*, 537 U.S. at 63 (nothing that "'a word is known by the company it keeps'" and, therefore, "the terms 'law' and 'regulation' used together in the pre-emption clause indicated that Congress pre-empted only positive enactments. If 'law' were read broadly so as to include the common law [when used in conjunction with regulation], it might also be interpreted to include regulations, which would render the express reference to 'regulation' in the pre-emption clause superfluous." (internal citations omitted)).

[46] In evaluating the express preemption clause of the Expedited Funds Availability Act (EFAA), which states that the EFAA "shall supersede any provision of the law of any State... which is inconsistent with this chapter," the U.S. Court of Appeals for the Ninth Circuit concluded that the plaintiff's common law claims were not preempted. Beffa v. Bank of the West, 152 F.3d 1174 (9th Cir. 1998). The court did not hold that the text of the EFAA clause applied only to positive law enactments and not common law claims. Instead, the court appeared to assume that the EFAA provision could preempt a common law claim if it fell within the subject matter of the clause and was inconsistent with the EFAA. In this case, the court simply determined that the claims being brought were outside the scope of the subject matter of the clause. *Id*. at 1177. *See also* Aresty Int'l Law Firm, P.C. v. Citibank, N.A., 677 F.3d 54 (1st Cir. 2012) (interpreting the EFAA express preemption clause and evaluating whether a common law claim fell within the subject matter of the clause). The U.S. Court of Appeals for the Second Circuit, in evaluating the effect of the Federal Election Campaign Act's (FECA) express preemption clause, undertook a similar analysis. Stern v. General Electric, Co., 924 F.2d 472 (2d Cir. 1991). That clause applies to "any provision of State law with respect to election to Federal office." 52 U.S.C. § 30143. The court found that the plaintiff's shareholder derivative suit was not preempted by FECA, not because the claims were not the *type* of claim that fell within the meaning of the clause, but because the claims were not within the subject matter of the clause. *Stern*, 924 F.2d at 475.

In non-preemption contexts, the Court has also interpreted the phrase "state law" to include both positive law enactments and common law claims. *See Cipollone*, 505 U.S. at 522; Norfolk & Western R. Co. v. Train Dispatchers, 499 U.S. 117, 128 (1991) (concluding that a federal law providing rail carriers with exemptions from "all other law, including state and municipal law" "does not admit of [a] distinction... between positive enactments and common-law rules of liability").

[47] *See supra* note 29 and accompanying text.

[48] One could argue, as the *Cipollone* Court noted, that even if "state law" has been interpreted broadly in other contexts so as to encompass common law claims, the presumption against preemption should counsel against such an interpretation in an express preemption context. *Cipollone*, 505 U.S. at 504 ("Although the presumption against pre-emption might give good reason to construe the phrase 'state law' in a pre-emption provision more narrowly than an identical phrase in another context, in this case such a construction is not appropriate.").

[49] Am. Airlines v. Wolens, 513 U.S. 219, 228 (1995); *see also Ginsberg*, 134 S. Ct. at 1431-33 (noting that whether a breach of implied covenant of good faith and fair dealing claim was preempted depended upon whether a state allowed parties to contract out of the covenant.).

obligations would likely not be considered a rule or standard enacted or enforced by the state and is unlikely to be preempted under these types of express preemption clauses.

A reviewing court may also need to delve into the elements of the common law action to determine if it satisfies all of the elements of an express preemption clause. For example, in *Bates v. Dow Agrosciences*, the Supreme Court concluded that an express warranty claim regarding a pesticide label was not preempted by a provision applying to "requirements for labeling or packaging."[50] The common law rule underlying the express warranty claim did not require the manufacturer to make an express warranty, it only required that the manufacturer "make good" on the commitment it voluntarily undertook. Therefore, even though losing such a claim would likely induce the manufacturer to change its label, the claim itself still did not constitute a requirement as contemplated by the preemption provision.[51]

Saving Clauses

As noted above, if a saving clause is present, it must be read in conjunction with an express preemption clause to determine what types of state actions will ultimately be superseded based on express preemption.

For example, an express preemption clause that preempts "any law, rule, regulation, duty, requirement, standard, or provision having the force and effect of law" would likely be interpreted as preempting state statutes, regulations, and common law causes of action. However, if that bill has a saving clause stating that the express preemption clause "shall not exempt a covered entity from liability under common law," the express preemption analysis changes.[52] Reading the express preemption and saving clauses together, it is likely that such a bill would be interpreted as expressly preempting state positive law enactments but not state common law causes of action. Saving clauses may also identify specific kinds of laws that are not to be preempted. For example, a saving clause may shield "state trespass, contract, or tort law" from express preemption.[53]

Ultimately, the existence of a saving clause can significantly change the scope of an express preemption clause and must be read in light of the plain text, express preemption clause, and the purpose of the statute as a whole.[54]

Subject Matter of Preempted Actions

Existing federal proposals vary in defining the subject matter of state actions to be preempted. Some bills define the subject matter of preempted actions narrowly, by preempting state statutes, regulations, and/or common law claims that "require" or "expressly require" certain actions.[55] For example, H.R. 580 preempts a state action that

> expressly—
>
> (1) requires information security practices and treatment of data containing personal information similar to any of those required under section 2; and

[50] Bates v. Dow Agrosciences, 544 U.S. 431, 443-46 (2005).

[51] *Id*. at 445.

[52] *See* H.R. 1770, § 6(b).

[53] *See, e.g.*, H.R. 580, § 6(c); S. 177, § 7(c).

[54] *See Geier*, 529 U.S. at 868.

[55] *E.g.*, H.R. 580, § 6; S. 177, § 7; S. 1158, § 220.

> (2) requires notification to individuals of a breach of security resulting in unauthorized access to or acquisition of data in electronic form containing personal information.[56]

This clause is likely to expressly preempt only state laws, regulations, and common law causes of action[57] that specifically impose data security and breach notification requirements. It is unlikely that this kind of provision would be interpreted to preempt general state consumer protection statutes, since these statutes would not "expressly require" certain conduct with regard to security and notification, but rather impose general standards of behavior to be applied to all situations.

Alternatively, several bills use the term "relating to" when describing the subject matter of express preemption.[58] For example, S. 1027 preempts state actions "relating to the protection or security of data in electronic form containing personal information or the notification of a breach of security."[59] Bills using the term "relating to" are likely to be interpreted as preempting a broader swath of state actions. The Supreme Court has described "relating to" within the context of express preemption clauses as broad and having an "expansive sweep." In *Morales v. TWA*, the Court determined that a provision preempting actions "relating to rate, routes, or services of any air carrier" superseded not only state laws that directly addressed air carriers but laws of general applicability, such as a consumer protection statute, when applied to air carriers.[60] Later cases importantly noted that "the breadth of the words 'related to' does not mean the sky is the limit"[61] and that such words should not be read "with an 'uncritical literalism.'"[62] For example, the Court has cautioned that an express preemption clause regarding motor carriers similar to the air carrier provision "does not preempt state laws affecting carrier prices, routes, or services 'in only a tenuous, remote, or peripheral ... manner.'"[63]

A bill that expressly preempts statutes and regulations "relating to" the protection or security of covered data or the notification of a breach of security[64] would clearly supersede state laws that directly address data security or notification, such as a statute establishing breach notification requirements. It would also likely preempt more general state laws, such as a consumer protection

---

[56] H.R. 580, § 6.

[57] This clause would only preempt common law causes of action that are not covered under the scope of its saving clause, which states: "This Act shall not be construed to preempt the applicability of—(1) State trespass, contract, or tort law; or (2) other State laws to the extent that those laws relate to acts of fraud." H.R. 580, § 6(c).

[58] *See, e.g.*, H.R. 1053, § 156; H.R. 1704, § 109; S. 547, § 156; S. 1027, § 8. Additionally, H.R. 1770 uses the term "relating to or with respect to." H.R. 1770, § 6(a).

[59] S. 1027, § 8.

[60] Morales v. TWA, 504 U.S. 374, 383-84 (1992) ("The ordinary meaning of these words is a broad one—'to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection with,'—and the words thus express a broad pre-emptive purpose. We have repeatedly recognized that in addressing the similarly worded pre-emption provision of the Employee Retirement Income Security Act of 1974 (ERISA)... which pre-empts all state laws 'insofar as they ... relate to any employee benefit plan.' We have said, for example, that the 'breadth of [that provision's] pre-emptive reach is apparent from [its] language,' ...; that it has a 'broad scope,'... and an 'expansive sweep,' ... ; and that it is 'broadly worded,'... 'deliberately expansive,'... and 'conspicuous for its breadth'"....). *See also Wolens*, 573 U.S. at 228. The Court later described the *Wolens* decision by stating: "The plaintiffs in that case sought to bring a claim under the Illinois Consumer Fraud and Deceptive Business Practices Act. Our conclusion that the state-law claim was pre-empted turned on the unusual breadth of the ADA's pre-emption provision, 'relating to rates, routes, or services,' is a broad one." *Good*, 555 U.S. at 85.

[61] Dan's City Used Cars, Inc. v. Pelkey, 133 S. Ct. 1769, 1778 (2013).

[62] *Id.* (quoting N.Y. State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co., 514 U.S. 645, 655-56 (1995)).

[63] *Id.* (quoting Rowe v. N.H. Motor Transp. Assn., 522 U.S. 364, 371 (2008)).

[64] *E.g.*, S. 1027, § 8.

law that prohibits unfair and deceptive acts or practices, because such a law would "relate to" data security and notification when it is applied to a data breach.

Finally, some bills use the phrase "with respect to" to describe the subject matter of preempted state actions. For example, H.R. 2205 preempts state actions

> with respect to the responsibilities of any person to—
>
> (1) protect the security of information relating to consumers that is maintained, communicated, or otherwise handled by, or on behalf of, the person;
>
> (2) safeguard information relating to consumers from—
>
> (A) unauthorized access; and
>
> (B) unauthorized acquisition;
>
> (3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or
>
> (4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.[65]

The courts have provided less guidance on the meaning of this phrase and it is unclear if the phrase is likely to be interpreted as similar to "relating to" or narrower in scope. Federal courts have considered at least one express preemption clause that uses "with respect to." The clause, from the Federal Election Campaign Act (FECA), preempted "any provision of state law with respect to election to federal office"[66] and has been interpreted relatively narrowly. The U.S. Court of Appeals for the Fifth Circuit found that the act did not preempt a claim based on a general state fraud statute. In reaching this conclusion, the court appeared to draw a distinction between statutes that specifically regulated federal elections, which would be preempted, and statutes of general applicability that could be applied to federal election activities, which would not be preempted.[67] However, it is unclear if the court's analysis was based strictly on a plain language interpretation or if it relied equally on the text and purpose of the overall legislative scheme.

If a federal law that preempted state statutes and regulations "with respect to" data security were interpreted narrowly, like the FECA provision, it likely would preempt state laws that establish data security standards, but would not preempt a general consumer protection statute. Alternatively, if the provision were interpreted more broadly, it could encompass both the direct data security laws as well as laws of general applicability, such as general consumer protection laws. In this instance, the statute's underlying congressional intent may help guide a court's interpretation of an arguably ambiguous express preemption clause.

[65] H.R. 2205, § 6. *See also* S. 961, § 6. Additionally, H.R. 1770 uses the term "relating to or with respect to." H.R. 1770, § 6(a).

[66] 52 U.S.C. § 30143.

[67] Janvey v. Democratic Senatorial Campaign Comm., Inc., 712 F.3d 185, 200-01 (5th Cir. 2013). Additionally, the U.S. Court of Appeals for the Second Circuit described the clause as containing "narrow wording" that "suggests that Congress did not intend to preempt state regulation with respect to non-election-related activities." *Stern*, 924 F.2d at 475.

Implied Conflict Preemption

The existence of an express preemption provision and/or a saving clause would not necessarily settle the question of the scope of potential preemption under a federal data security and breach notification statute. The Supreme Court has "made clear that the existence of a separate [express] pre-emption provision 'does not bar the ordinary working of conflict pre-emption principles.'"[68] Therefore, after determining the scope of express preemption, a reviewing court may then need to determine if state actions that would not be expressly preempted may, nonetheless, be preempted under principles of implied conflict preemption.[69]

Conflict preemption can be present in two instances: first, where compliance with both the state and federal law is a physical impossibility (impossibility preemption)[70] and second, when the state action "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress"[71] (obstacle preemption).

Impossibility Preemption

Impossibility preemption has previously been described by the Supreme Court as a situation in which a state law prohibits what the federal law requires, or vice versa.[72] Generally, it requires the presence of conflicting affirmative legal obligations imposed by state and federal law. For example, the Supreme Court provided a useful illustration of these principles in *Florida Lime & Avocado Growers v. Paul*.[73] In a hypothetical it constructed, the Court noted that a state law preventing the picking and marketing of avocados testing less than 8% of oil would be preempted under impossibility preemption if a federal law forbade the picking and marketing of avocados testing more than 7% oil.[74]

However, where a state or federal law simply permits an activity the other restricts or prohibits, impossibility preemption appears not to apply.[75] Commentators have suggested that instances of impossibility preemption are relatively rare.[76]

---

[68] Hillman v. Maretta, 133 S. Ct. 1943, 1954 (2013) (citing *Sprietsma*, 537 U.S. at 65).

[69] Implied preemption can also occur when a "scheme of federal regulation is so pervasive as to make reasonable the inference that Congress left no room for the states to supplement it." *Rice*, 331 U.S. at 230. This type of implied preemption is called field preemption, because Congress has occupied the field within the given subject area such that states may not regulate. This type of preemption is not addressed in this report.

[70] Florida Lime & Avocado Growers v. Paul, 373 U.S. 132, 142-43 (1963).

[71] Hines v. Davidowitz, 312 U.S. 52, 67 (1941).

[72] The Court has noted that impossibility preemption is a "demanding defense." *Wyeth*, 555 U.S. at 573.

[73] *Paul*, 373 U.S. at 143.

[74] *Id*.

[75] *See Wyeth*, 555 U.S. at 571-72 (finding that impossibility preemption did not exist because state law required the drug manufacturer to add an adequate warning about the risk of IV-push administration and that federal law permitted the manufacturer to make such a label change before the FDA approved it); Barnett Bank v. Nelson, 517 U.S. 25, 31 (1996) (noting that the two statutes at issues in the case "do not impose directly conflicting duties on national banks—as they would, for example, if the federal law said, 'you must sell insurance,' while the state law said, 'you may not'"). In *Mutual Pharmaceutical Company v. Bartlett*, the Supreme Court held that a state tort defective design claim against a generic drug manufacturer was preempted by federal law due to impossibility preemption. Mutual Pharm. Co. v. Bartlett, 133 S. Ct. 2466 (2013). The Court concluded that the state common law required the manufacturer to strengthen the warnings on the drug's label. *Id*. at 2475. However, the manufacturer was prohibited under federal law from changing the label. *Id*. at 2476. Therefore, since the state law required action that the federal law prohibited, compliance with both was impossible. *Id*. at 2477. The Court rejected the lower court's finding that impossibility preemption should not apply because the drug manufacturer could choose to stop selling the drug altogether. If such a (continued...)

To illustrate the application of impossibility preemption, consider a hypothetical federal law that expressly preempts less stringent state data breach notification laws, thereby setting a floor for minimum protection but allowing states to impose stricter standards.[77] The federal standard requires covered entities to notify affected persons as expediently as possible and generally within 30 days of discovering a breach, but also provides exceptions under which notification would be delayed, for example if it would impede a criminal investigation or for national security reasons.[78] A state data breach notification statute that imposed more stringent requirements than the federal law would survive under an express preemption analysis but could still be superseded due to impossibility preemption. Under the state statute, a covered entity must delay notification to the affected parties if it would impede a criminal or civil investigation.[79] Assume a covered entity experiences a data breach that triggers both state and federal notification requirements and that notification of that breach would impede a civil investigation. Under the state statute described, the covered entity would be prohibited from providing notice to the affected parties until cleared by law enforcement. However, under the federal law described, which does not allow for delayed notification because of an ongoing civil investigation, the entity would be required to provide notice within 30 days. Since the federal law requires the entity to take action that is prohibited under state law, compliance with both laws would be impossible. Therefore, a reviewing court is likely to conclude that the state law is preempted under impossibility preemption.

Obstacle Preemption

Obstacle preemption analysis is broader in scope. In determining when a state action "stands as an obstacle," a reviewing court must consider congressional intent and the "purposes and objectives" of the federal statute as a whole.[80] "If the purpose of the act cannot otherwise be accomplished," the Supreme Court has held, then "the state law must yield to the regulation of Congress.... "[81] Obstacle preemption can be difficult to apply, since it relies heavily on a reviewing court's interpretation of Congress's purposes in creating the legislative scheme at issue and may require a nuanced analysis of the applicable state law.

(...continued)

theory were accepted, the Court concluded that "impossibility preemption would be 'all but meaningless.'" *Id*. Justice Sotomayor's dissent disagreed with the majority's reasoning because she found that the state common law did not create a requirement for the manufacturer to change the drug's label. Instead, she characterized the tort action as creating an incentive for the manufacturer to take certain action to avoid future liability, but not an actual legal mandate. *Id*. at 2488-89 (Sotomayor, J., dissenting).

[76] Kerry Abrams, *Plenary Power Preemption*, 99 VA. L. REV. 601, 608-09 (2013).

[77] *E.g.*, S. 1158, § 220(a)-(b).

[78] *E.g.*, H.R. 1053, § 142(f); H.R. 1704, § 101(d); S. 1158, § 211(d).

[79] At least five state have data breach notification statutes that require delay of notification if it will jeopardize a civil investigation. *See, e.g.*, N.J. STAT. ANN. § 56:8-163(c)(2); OKLA. STAT. tit. 24, § 163(D); 73 PA. CONS. STAT. § 2304; VA. CODE ANN. § 18.2-186.6; W. VA. CODE § 46A-2A-102(e).

[80] *Crosby*, 530 U.S. at 373 (noting that in considering obstacle preemption, a court's judgment is to be informed by "examining the federal statute as a whole and identifying its purpose and intended effects").

[81] *Id*. *Geier* provides an example of obstacle preemption when an express preemption clause is also present. In that case, the Supreme Court held that a plaintiff's state tort claim, which was based on the theory that an automobile manufacturer had a duty under common law to install an airbag in its manufactured vehicles, was preempted. *Geier*, 529 U.S. at 874. Because the applicable federal law had the objective of ensuring a variety of passive restraint systems, just one of which was airbags, the state common law claim would have presented an obstacle to the accomplishment of this purpose. *Id*. at 881.

Consequently, proposals that focus on creating a uniform, nationwide standard for data security and breach notification[82] are more likely to supersede state law under obstacle preemption—since the existence of individual state standards would prohibit national uniformity—than a federal law that instead focused on setting minimum national standards.

Determining whether a state common law cause of action that remains valid after an express preemption analysis would still be superseded under obstacle preemption can be particularly difficult. The outcome of such an analysis may depend upon how a reviewing court interprets the elements of the claim under state law and the precise purpose of the federal law. The Supreme Court confronted this kind of question regarding the nature of a state tort claim in *Mutual Pharmaceutical Company, Inc. v. Bartlett*.[83] In that case, the Court had to determine whether a New Hampshire tort design-defect claim was preempted by federal law under impossibility preemption. In discussing the specifics of the claim, the five Justices of the majority determined that the state tort cause of action imposed a duty on the defendant to take a specific remedial action and, therefore, was preempted.[84] However, two Justices writing in dissent argued that the state tort law did not impose an affirmative legal obligation on the defendant to take the remedial action. Instead, they stated that the claim "create[d] an incentive" for the defendant or similar entities to make changes to their products "to try to avoid liability."[85] This case highlights the complexity of this analysis, which depends on a court's interpretation of the specific elements of the state common law claim, and the possibility that judges may come to differing conclusions about the proper analysis of a specific claim.

Similarly, a reviewing court could view a negligence claim, if successful, as creating a legal duty for the defendant to implement better data security practices, including potentially a specific type of security mechanism. Under this view, the defendant and similarly situated entities in that state would then be subject to a legal requirement imposed by state common law to adopt those security practices, which a review court may determine to be in conflict with a federal law whose purpose is to create one uniform standard nationwide. Alternatively, a reviewing court might view that common law negligence claim as simply a request by the plaintiffs to be compensated for their injuries. Under this interpretation, the claim may not be in conflict with a federal law that seeks uniformity, since it would not impose an affirmative legal obligation on the defendant to take specific actions to cure its data security defects, but would simply require that the defendant compensate the plaintiffs.

[82] The purpose of the federal law may be included in a purposes section of the text itself. *.g.*, H.R. 1770, § 1(b) (stating the purposes of the bill). These purposes were reinforced by statements made by the Committee on Energy and Commerce as it considered the bill. *See* House Committee on Energy and Commerce, "Data Security and Breach Notification Act of 2015," March 25, 2015, https://energycommerce.house.gov/fact-sheet/data-security-and-breach-notification-act-2015 (noting that the law would create a "uniform national policy" that would "replac[e] the patchwork of state and territory laws" currently in place).

[83] 133 S. Ct. 2466 (2013).

[84] *Id*. at 2479-80.

[85] *Id.* at 2488 (Sotomayor, J., dissenting).

Key Takeaways on Federal Preemption of State Data Security and Breach Notification Laws

- Congress can supersede state and local laws, regulations, and common law causes of action through express preemption and/or implied preemption.
- Under express preemption, a reviewing court will closely examine the text of the express preemption clause to determine the *types* of actions that could be preempted and the *subject matter* scope of that preemption.
- All of the data security and breach notification bills include an express preemption clause.
- The text of the express preemption clause and a saving clause, if present, will determine whether state statutes, regulations, and common law causes of action regarding data security and breach notification specifically and/or consumer protection generally would be preempted.
- Even if there is an express preemption clause, state and local actions can still be superseded under implied conflict preemption.

Agency Enforcement of Data Security and Breach Notification Requirements

Another question that has arisen in the debate on federal data security and breach legislation is which federal agency should be responsible for enforcing the new requirements. The various proposals would primarily task the Federal Trade Commission (FTC) with enforcing the new requirements, but take differing approaches as to whether the Federal Communications Commission (FCC) should be permitted to retain its existing enforcement authority regarding data security and breach notification for telecommunication providers.

Current FTC Authority: Unfair or Deceptive Acts and Practices

The FTC has broad authority under Section 5 of the Federal Trade Commission Act (FTCA) to prohibit "unfair or deceptive acts or practices in or affecting commerce.... "[86] Under the statute, an act or practice may be unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[87] While the FTC's authority over unfair or deceptive practices is broad, it is not unlimited. For example, the FTC cannot use this authority to enforce against all "persons, partnerships, or corporations.... " Rather, several entities are exempted from the scope of this authority,[88] including

- banks and savings and loan institutions described in 15 U.S.C. § 57a(f)(3);
- federal credit unions described in 15 U.S.C. § 57a(f)(4);
- common carriers subject to the Communications Act of 1934, as amended;[89]
- common carriers subject to subtitle IV of title 49;[90]

[86] 15 U.S.C. § 45(a).

[87] 15 U.S.C. § 45(n).

[88] 15 U.S.C. § 45(a)(2).

[89] 47 U.S.C. §§ 151 *et seq.* Section 5 of the FTCA exempts "common carriers subject to the Acts to regulate commerce." 15 U.S.C. § 45(a)(2). Section 4 of the FTCA defines "Acts to regulate commerce" to include "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto." 15 U.S.C. § 44.

- air carriers and foreign air carriers subject to part A of subtitle VII of title 49;[91] and
- persons, partnerships, or corporations subject to the Packers and Stockyards Act.[92]

Therefore, for example, the FTC could not bring an enforcement action alleging an unfair or deceptive act or practice, engaged in as part of its common carrier activities, against a telephone company that is classified as a common carrier by the FCC under the Communications Act.

The FTC has employed its unfair or deceptive act or practice authority to bring enforcement actions and to seek settlements with companies that experience data breaches. These actions generally focus on the allegedly deceptive nature of the claims companies make about the security provided for consumers' data and/or the company's failure to reasonably safeguard consumer data that leads to a breach. For more information on the FTC's use of this authority in the data security and breach context, see CRS Report R43723, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, by Gina Stevens.

Current FCC Authority

While telecommunications common carriers are not subject to the FTC's unfair or deceptive acts or practices authority, they are required to follow FCC rules relating to data security and breach notification.[93] Section 222 of the Communications Act establishes a duty for common carriers "to protect the confidentiality of proprietary information of... customers.... "[94] Furthermore, under Section 201 of the Communications Act, common carriers must ensure that all "charges, practices, classifications, and regulations" relating to telecommunications service are just and reasonable, which the FCC has interpreted as applying to carriers' practices of protecting customers' personally identifiable information.[95]

Additionally, Sections 631[96] and 338(i)[97] of the Communications Act establish more limited security rights for subscribers of cable and satellite television providers, as discussed below.

(...continued)

[90] 49 U.S.C. §§ 10101 *et seq.* Section 5 of the FTCA exempts "common carriers subject to the Acts to regulate commerce." 15 U.S.C. § 45(a)(2). Section 4 of the FTCA defines "Acts to regulate commerce" to include "subtitle IV of title 49." 15 U.S.C. § 44.

[91] 49 U.S.C. §§ 40101 *et seq.*

[92] 7 U.S.C. §§ 181 *et seq.*

[93] Additionally, the FTC and FCC have recently signed a Memorandum of Understanding to coordinate the agencies' activities with regard to consumer protection. FCC-FTC Consumer Protection Memorandum of Understanding, Nov. 16, 2015, http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf.

[94] 47 U.S.C. § 222(a).

[95] 47 U.S.C. § 201(b); *see* In the Matter of AT&T Services, Inc., 30 FCC Rcd 2808 (April 8, 2015) *available at* https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches [hereinafter AT&T Consent Decree].

[96] 47 U.S.C. § 551.

[97] 47 U.S.C. § 338(i).

Common Carriers

Section 201(b) and 222 requirements apply to entities that are classified as common carriers under Title II of the Communications Act, which includes traditional telecommunications common carriers (such as telephone companies). Following the FCC's 2015 Open Internet Order,[98] in which the Commission reclassified broadband Internet access service providers (BIAS or Internet service providers) as Title II common carriers, these sections also apply to those entities, provided that the FCC's reclassification decision survives legal challenge.[99] For more information on the 2015 Open Internet Order, see CRS Report R43971, *Net Neutrality: Selected Legal Issues Raised by the FCC's 2015 Open Internet Order*, by Kathleen Ann Ruane.

Section 222 Customer Proprietary Network Information (CPNI)

Common carriers are subject to obligations derived from Section 222 of the Communications Act, which requires them to guard the confidentiality of customer proprietary network information (CPNI) and ensure that it is not disclosed to third parties without customer approval or as required by law.[100] CPNI is defined as

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
>
> except that such term does not include subscriber list information.[101]

It includes such information as call records, location information, features of a customer's service, and billing records, among other types of data.

The FCC has issued regulations explaining common carriers' duties to protect CPNI.[102] These regulations define when a carrier is permitted to use and/or share CPNI with other entities without a customer's approval and when a carrier can only use and/or share CPNI subject to a customer's

[98] In the Matter of Protecting and Promoting the Open Internet, Report and Order, FCC 15-24 (2015). The Order was subsequently published in the *Federal Register*. Protecting and Promoting the Open Internet, 80 Fed. Reg. 19737 (April 13, 2015).

[99] Numerous parties have challenged the FCC's 2015 Open Internet Order. Those cases have been consolidated in the U.S. Court of Appeals for the D.C. Circuit under the caption *United States Telecomm. Ass'n, et. al v. Federal Communications Commission*. U.S. Telecomm. Ass'n v. FCC, D.C. Cir. No. 15-1063. The Federal Register publication of the Order indicated that it would take effect on June 12, 2015. 80 Fed. Reg. 19738. Parties challenging the order filed a motion with the appellate court to stay the effective date of the order pending review. The court of appeals denied that motion, allowing the new rules to take effect on June 12. U.S. Telecomm. Ass'n v. FCC, D.C. Cir. No. 15-1063, Order Denying Motion for Stay and Granting Motion for Expedited Review (June 11, 2015), *available at* http://docs.techfreedom.org/oiostaydenial.pdf.

Assuming the Order survives legal challenges, by reclassifying BIAS as Title II common carriers, it appears as though the FTC will no longer have jurisdiction to enforce its unfair or deceptive acts or practices authority against these providers.

[100] 47 U.S.C. § 222.

[101] 47 U.S.C. § 222(h)(1).

[102] 47 C.F.R. §§ 64.2001 *et seq.*

opt-in or opt-out approval.[103] Carriers are also required to notify law enforcement and customers when a breach of CPNI occurs.[104]

In its Open Internet Order, the FCC specifically declined to forbear from applying Section 222 to Internet service providers, stating:

> We find that forbearance from the application of section 222 with respect to broadband Internet access service is not in the public interest... and that section 222 remains necessary for the protection of consumers... The Commission has emphasized that '[c]onsumers' privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services.'[105]

While the *statutory* requirements of Section 222 apply to Internet service providers, the FCC did choose to forbear from applying its CPNI *rules* to Internet service providers.[106] The Commission noted that the rules would not necessarily "be well suited to broadband Internet access service" since "certain of those rules appear more focused on concerns that have been associated with voice service ... [and] do not address many of the types of sensitive information to which a provider of broadband Internet access service is likely to have access."[107] However, the Commission stressed that Internet service providers must still comply with the text of the statutory provisions in Section 222.[108]

Section 201(b) Reasonableness Requirements

The FCC has also relied on its Section 201(b) authority to bring enforcement actions against common carriers that suffer data breaches. Section 201(b) states that common carrier "charges, practices, classifications, and regulations" must be just and reasonable.[109] For example, in 2015, the FCC entered into a consent decree with AT&T following an investigation into the company's alleged failure to protect the confidentiality of CPNI that led to a data breach.[110] The FCC declared that AT&T's "failure to reasonably secure" CPNI not only violated its duties under Section 222 but "also constitute[d] an unjust and unreasonable practice in violation of the [Communications] Act."[111] It referenced an earlier enforcement action in which the FCC determined that a "failure to protect and secure" customers' personally identifiable information, CPNI, and other kinds of data, was an unjust and unreasonable practice in violation of Section 201(b).[112] This failure was evidenced in part by the fact that the carrier did not encrypt any of its customers' data that was stored on servers accessible over the public Internet.[113] Along with Section 222, Section 201(b)'s reasonableness requirement appears to be another tool the FCC can use to hold carriers accountable for certain data security and breach failures.

---

[103] 47 C.F.R. §§ 64.2005, 64.2007.

[104] 47 C.F.R. § 64.2011.

[105] 80 Fed. Reg. 19814.

[106] 80 Fed. Reg. 19815.

[107] *Id*.

[108] 80 Fed. Reg. 19814-19815.

[109] 47 U.S.C. § 201(b).

[110] AT&T Consent Decree, *supra* note 95, at 2808.

[111] *Id*.

[112] In the Matter of TerraCom, Inc. and YourTel America, Inc. Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13335-36 (2014).

[113] *Id*. at 13336.

Cable and Satellite Providers

Several statutory provisions also impose data security requirements on cable and satellite television providers. Section 631 of the Communications Act prohibits a cable operator from using a cable system "to collect personally identifiable information concerning a subscriber without the prior written or electronic consent of the subscriber concerned."[114] Furthermore, cable operators are forbidden from disclosing a subscriber's personally identifiable information without the subscriber's consent (with limited exceptions) and must "take such actions as are necessary to prevent unauthorized access to such information" by a third party.[115] Similar provisions apply to satellite television carriers.[116] These data security requirements for cable and satellite operators include protections for a subscriber's viewing history.[117]

Key Takeaways on Agency Enforcement Roles

- Both the FTC and the FCC have interpreted their statutory authority to permit enforcement actions against entities that have poor data security practices and experience data breaches.
- The FTC brings enforcement actions under its "unfair or deceptive acts or practices" authority in the FTC Act. However, this authority does not allow the FTC to bring enforcement actions against common carriers (as classified by the FCC under the Communications Act) that experience data breaches while engaging in common carrier activities.
- The FCC brings enforcement actions against common carriers under its rules for protecting customer proprietary network information (CPNI) and a provision of the Communications Act that requires "charges, practices, classifications, and regulations" to be just and reasonable.
- The FCC also has rules governing the disclosure of customer information that apply to cable and satellite providers.
- Several data security and breach notification bills would alter these existing authorities—either expanding the FTC's authority to include common carriers and eliminating the FCC's authority or expanding the FTC's authority while leaving the FCC's rules untouched.

Proposed Changes to FTC and FCC Enforcement Authority

Several of the bills being considered in the 114th Congress propose changes to the FTC and FCC's existing enforcement authority regarding data security and/or breach notification, while two others would leave the current system essentially unaltered.[118] Under the bills that propose no changes to enforcement authority, common carriers under the Communications Act would not be

[114] 47 U.S.C. § 551(b).

[115] 47 U.S.C. § 551(c). The FCC recently entered into a consent decree with Cox Communications, Inc., representing its first enforcement action against a cable operator regarding a data breach. In the Matter of Cox Communications, Inc., 2015 FCC LEXIS 3412 (Nov. 5, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1241A1.pdf.

[116] 47 U.S.C. § 338(i).

[117] 47 U.S.C. §§ 338(i)(4)(B)(iii), 551(c)(2)(C). A person aggrieved by a violation of section 631 or 338(i) may bring a civil action in a federal district court seeking actual damages, punitive damages, and attorneys' fees. 47 U.S.C. §§ 338(i)(7), 551(f).

[118] H.R. 580 and S. 177 make requirements for data security and breach notification applicable only to those entities already subject to FTC unfair and deceptive acts or practices enforcement, with limited exceptions. H.R. 580, § 4(a)-(b); S. 177, § 5(a), (c). S. 177 applies its new requirements to non-profit entities, notwithstanding the existing limits on FTC enforcement authority in 15 U.S.C. §§ 44, 45(a)(2). S. 177, § 5(a)(2). It also includes an "opt-in" provision that would allow entities that are not automatically covered to voluntarily enter into an agreement with the FTC to be bound by the bill's breach notification requirements. *Id*. at § 5(b).

subject to new data security and breach notification requirements, since they are not subject to FTC unfair or deceptive acts or practices authority. Common carriers would continue to be subject to Sections 201(b) and 222, as enforced by the FCC. Alternatively, cable and satellite providers would be subject to both the bills' new requirements, because they fall within the FTC's unfair or deceptive acts or practices authority, and Section 338(i) or 631, as applicable.

Some of the bills that propose changes to the current agency enforcement structure would expand the FTC's jurisdiction and leave the FCC's existing statutory and regulatory authority intact.[119] For example, under H.R. 1704, the FTC would enforce the new requirements "in the same manner, by the same means, and with the same jurisdiction, powers, and duties" as it has under the FTCA, except that the exceptions to its Section 5 authority "shall not apply."[120] The bill does not alter the FCC's authority under Sections 201, 222, 338(i), or 631, although it does require the FTC to consult with the FCC before promulgating rules regarding an entity within the FCC's jurisdiction.[121] If this type of bill were enacted, common carriers and cable and satellite providers would all be subject to both the new requirements in the bill, as enforced by the FTC, and the FCC's existing requirements.

Alternatively, some bills both expand the FTC's jurisdiction and eliminate some or all of the FCC's authority to regulate in this area.[122] For example, H.R. 1770 states that,

> as sections 201, 202, 222, 338, and 631 of the Communications Act of 1934... and any regulations promulgated thereunder, apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information, such sections and regulations promulgated thereunder *shall have no force or effect*, unless such regulations pertain solely to 9–1–1 calls.[123]

Under this bill, with the exception of regulations pertaining solely to 911 calls, the FCC retains no authority to enforce its requirements under Sections 201, 222, 338, and 631.[124] Therefore, if this type of bill were enacted, common carriers and cable and satellite providers would be subject to the new requirements, as enforced by the FTC, but would no longer have to comply with the FCC requirements. Other bills only eliminate the FCC's ability to enforce *some* of the relevant Communications Act provisions regarding data security and breach notification, but not all.[125]

---

[119] *E.g.*, H.R. 1704, § 107; S. 1158, §§ 203(d), 218(d). H.R. 1704 also requires the FTC to consult with the FCC if its enforcement action involves a business entity subject to the FCC's authority. H.R. 1704, § 107(c). S. 1158 specifically preserves the FCC's authority by stating that "[n]othing in this Act may be construed in any way to limit the authority of the Federal Communications Commission under any other provision of law." S. 1158, § 220(e).

[120] H.R. 1704, § 107(b).

[121] *Id*. at § 107(f)(2).

[122] H.R. 1053, § 171(c); H.R. 1770, § 6(c); H.R. 2205, § 5(b); S. 547, § 171(c); S. 961, § 5(b); S. 1027, § 4(b).

[123] H.R. 1770, § 6(c)(1) (emphasis added).

[124] *Id*.

[125] H.R. 1053 and S. 547 state that "If a person is subject to a provision of section 222 or 631 of the Communications Act of 1934... and a provision of this title, such provision of such section 222 or 631 shall not apply to such person to the extent that such provision of this title applies to such person." H.R. 1053, § 171(c); S. 547, § 171(c). These bills do not appear to alter the validity of Sections 201 or 338 of the Communications Act. S. 1027 states that "Sections 222, 338, and 631 of the Communications Act of 1934... and any regulations promulgated thereunder, shall not apply with respect to the information security practices, including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections." S. 1027, § 4(b). This bill does not appear to alter the validity of Section 201 of the Communications Act.

Removing the FCC's authority in this area may reduce the types of data that are subject to security and breach notification requirements, as compared with a proposal that imposes new requirements while maintaining the FCC's authority. For example, data within the existing definition of CPNI may not meet the definition of "covered information" in the federal proposal, and, therefore, may not be subject to the new federal standards nor the security and breach notification requirements in the CPNI rules, if those rules have "no force or effect" going forward.

Proponents of bills that reduce or eliminate the FCC's authority in this subject area have emphasized the benefits of imposing a uniform, predictable standard across all covered entities.[126] Opponents of this approach argue that restricting FCC authority weakens consumer protection by eliminating clear, predictable rules with which companies are accustomed to complying.[127] Some also argue that the type of data to be protected under new federal requirements would be more limited than the data protected under the Communications Act provisions and, therefore, eliminating the FCC's ability to enforce those provisions will reduce consumers' data protection.[128] These issues are likely to continue to be discussed as the bills are considered in the 114th Congress.

Author Contact Information

Alissa M. Dolan
Legislative Attorney
adolan@crs.loc.gov, 7-8433

[126] *See* House Energy and Commerce Committee, "Data Security and Breach Notification Act of 2015," March 25, 2015, *available at* http://energycommerce.house.gov/fact-sheet/data-security-and-breach-notification-act-2015 (noting that the draft bill that eventually became H.R. 1770 is "designed to create a uniform national policy ... ").

[127] Testimony of Laura Moy, Senior Policy Counsel, New America's Open Technology Institute, Before the House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade, "Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015," March 18, 2015, *available at* http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf ("The FCC's robust rules promulgated under that authority require telecommunications carriers to, among other things, train personnel on customer proprietary network information (CPNI), have an express disciplinary process in place for abuses, and annually certify that they are in compliance with the CPNI rules... [T]he specific data security requirements imposed by the FCC[] would all be eliminated by this bill and replaced with the less specific 'reasonableness' standard... The consumer protections provided by the Communications Act are of critical importance to consumers, and appropriately overseen by an agency with decades of experience regulating entities that serve as gatekeepers to essential communications networks. This bill threatens to eliminate core components of those protections.... " (internal citations omitted)).

[128] Letter to Chairman Fred Upton and Ranking Member Frank Pallone from numerous consumer groups, Re: the Data Security and Breach Notification Act (H.R. 1770), *available at* http://www.consumerfed.org/pdfs/150409_Data-Security-Breach_letter.pdf. The letter argues that

> The Communications Act contains very strong data security and breach notification protections for information about customers' use of telecommunications services. It also protects cable and satellite subscribers' information, including their viewing histories. But as with email login information and health records, this bill is too narrow to cover all telecommunications usage information, and it would not protect cable and satellite viewing histories at all. The bill would simply eliminate data security and breach notification protections for sensitive information about use of these services. In addition, the breach notification and data security protections in this bill are weaker than existing law under the Communications Act.

Id. at 2.