Bloomberg Law Reports® Technology Law

From Pickpockets to Playstations: Evolving Data Privacy Threats and Federal and State Responses

Elizabeth McGinn, Sasha Leonhardt, and Gastón Kuperschmit, BuckleySandler LLP

Abstract

In recent years, there have been several high-profile security breaches relating to consumer financial data. These breaches – involving companies as diverse as GE Money, AOL, T.J. Maxx, Boeing, Rite Aid, and most recently, Sony's PlayStation Network – have revealed the personal information of hundreds of millions of consumers. In response to these events, members of Congress have proposed several bills to give the Federal Trade Commission the authority to craft regulations and administer penalties for breaches of data security. While Congress is just now making serious progress towards a legislative solution to this issue, the FTC and individual states have been struggling with data breaches for some time. This article reviews the current patchwork of federal and state data breach laws and enforcement actions regarding data breaches and then considers several bills before Congress that attempt to create a national data privacy standard.

Introduction

In April 2011, Sony's PlayStation Network made worldwide headlines when computer hackers compromised sensitive personal and financial data for more than 100 million customer accounts.[1] One analyst estimates the potential loss to Sony at a staggering $24 billion dollars.[2] Although this is the most sensational breach of consumer financial data to date, it is certainly not the first. In 2006, an unencrypted laptop was stolen from a Boeing employee's car; the laptop contained Social Security numbers, names, and home addresses of 382,000 former and current employees.[3] That same year, a careless AOL employee posted a data file with 20 million allegedly anonymous Internet searches on it; however, a data breach occurred because AOL customers had been using their names, addresses, and Social Security numbers as search strings.[4] In 2007, GE Money's loss of a single magnetic backup tape threatened the personal information of 650,000 individuals.[5] Later that year, TJX – the parent company of retailers T.J. Maxx and Marshalls – announced that a data breach may have revealed more than 45 million credit and debit card numbers with an estimated cost to TJX of $4.5 billion.[6] In 2009, a single data breach at Heartland Payment Systems exposed 130 million credit card numbers to hackers.[7] Estimates at the time put the cost of this data breach at $140 million.[8] In 2010, Rite Aid paid $1 million to settle a complaint by the Federal Trade Commission ("FTC") that the pharmacy's employees were systematically leaving confidential patient information in open, unsecured dumpsters.[9]

As data breaches become an inevitable risk for any modern business, there are few laws outlining a business's legal responsibility in these situations.[10] The FTC has taken the de facto lead on the issue of data security through its broad – yet unspecified –

administrative authority to punish unfair and deceptive acts and practices ("UDAP") under the FTC Act.[11] To fill this statutory gap, several states have passed their own data breach laws to protect consumers. However, most data breaches have affected consumers on a nationwide – rather than individual state – basis. Without a national standard, these diverse state laws create inefficiency and uncertainty for companies that are attempting to follow the law in good faith and protect their customers' data.

Recognizing this situation, members of Congress have proposed several bills to confront these pressing data security issues. While the substance of these bills differs significantly, it is clear that Congress intends to preempt state laws and create a single, national standard for data security.

Current Federal Privacy Law: Recent FTC Enforcement Actions

Today, FTC is the primary enforcer of federal commercial privacy laws. The FTC's main tool to protect consumer data is Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices in commerce.[12] When the FTC Act was passed in 1914 – in a time long before Social Security numbers and IP addresses – Congress could not have anticipated the international exposure of millions of Americans' personal data.[13] The FTC's pre-2005 data breach complaints relied solely upon instances when a business failed to act in accordance with representations made in its privacy policy or marketing materials.[14] Recently, however, the FTC has broadened its complaints to include companies' failure to employ reasonable and appropriate measures to secure personal information.[15]

In May 2011, the FTC initiated enforcement actions against two companies that provide human resource support, Ceridian Corp. ("Ceridian")andLookout Services, Inc. ("Lookout"), alleging UDAP violations.[16] In both cases, the FTC alleges that the companies violated the FTC Act both by not having reasonable and adequate security protocols and by falsely stating that they had reasonable and appropriate security procedures in place to protect the personal data of their clients' employees.[17] The lack of adequate security made it easier for unauthorized individuals to discover the names, addresses, e-mail addresses, telephone numbers, Social Security numbers, birthdates, and direct deposit account numbers of over 60,000 individuals.[18] The FTC was particularly concerned that many of these individuals may become the eventual victims of identity theft. [19]

The draft complaint against Ceridian alleges thatthe company engaged in several practices that, as a whole, failed to provide adequate security for customers' personal information. These alleged practices include: (1) storing information in clear, readable text; (2) creating unnecessary risks by storing personal information indefinitely without a business need; (3) failing to assess the vulnerability of its systems to reasonably foreseeable attacks; (4) failing to implement readily available, free or low-cost defenses to such attacks; and (5) failing to employ reasonable measures to detect and prevent unauthorized access to personal information.[20] The FTC describes these practices as "fundamental security failures" and notes that each has been challenged in prior data security cases.[21]

Similarly, the draft complaint against Lookout alleges that it engaged in various practices that together failed to provide reasonable and appropriate security for personal information. These practices include: (1) failing to implement reasonable policies and procedures for securing sensitive information; (2) failing to establish or enforce rules to make user credentials (i.e. user IDs and passwords) difficult to guess; (3) failing to require periodic changes of user credentials; (4) failing to suspend user accounts after repeated unsuccessful login attempts; (5) failing to address widely-known security flaws such as "predictable resource location" which enables users to predict Internet links to secure web pages; (6) allowing users to bypass authentication procedures

if they typed in a specific URL; (7) failing to employ sufficient measures to detect and prevent unauthorized access to data such as an intrusion detection system and system logs; and (8) storing database passwords in unencrypted text.[22]

In both cases, the FTC has proposed consent decrees that are designed to protect consumers' and employees' personal information. As a nod to the statutory UDAP basis of the FTC's authority, the proposed consent decrees each begin with a boilerplate, one-sentence prohibition against misrepresentations about the security of consumers' personal information.[23] The consent decrees then move beyond core UDAP concerns and require the companies to maintain comprehensive information security programs that are reasonably designed to protect consumers' personal information.[24] Specifically, the consent decrees require these security programs to contain appropriate administrative, technical, and physical safeguards;[25] obligate both companies to obtain independent security audits every other year for 20 years;[26] and impose reporting and compliance provisions.[27]

The Ceridian and Lookout complaints demonstrate that the FTC is attempting to expand its authority within the statutory constraints of the FTC Act's UDAP provisions. Although each complaint makes a glancing reference to the companies' representations – and each consent order includes a cursory UDAP paragraph – the consent decrees go far beyond UDAP in requiring the creation of an entire data security structure. In so doing, the FTC is struggling to remain faithful to its statutory mission while filling a void left by the absence of a comprehensive data security law.

Current Privacy Law: State Legislation

With no federal legislation to govern data breaches, individual states have stepped into this void and passed their own laws to protect individual consumers from data privacy violations. To date, 46 states and the District of Columbia have passed some form of data breach legislation.[28] Of these states, two stand out as deserving in-depth analysis: California and Massachusetts. As the first state to pass a data breach law, California has framed the data security debate and serves as a model for the majority of other states' data security legislation.[29] Massachusetts represents the next step in data protection law by giving an administrative body the power to create detailed regulations to protect consumer information.

California

California was the first state to enact legislation to protect personal information. In 2003, California enacted Cal. Civ. Code § 1798.82 which requires companies that retain customer data electronically to notify their California customers of a security breach. This legislation applies to all companies conducting business in California, even if the data breach occurs outside of the state. The law protects personal data including the customer's name, Social Security number, and account numbers.[30] If such information is obtained by an unauthorized party, the business must provide notice to all affected individuals.[31] If the data breach is significant – if providing notice would cost more than $250,000, there are more than 500,000 California residents affected, or there is insufficient contact information for affected customers – notification may be accomplished by e-mail, a posting on the business's website, and through state-wide media.[32]

To augment its data protection laws, the California legislature enacted Cal. Civ. Code § 1798.81.5 in 2004. The 2004 law requires any business that maintains personal information to "implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[33] While California law does not define a "reasonable security procedure," the law does require that such procedures be proportionate to the type of data maintained.

In 2009 and 2010, California legislators attempted to expand its data breach laws. Both years, the legislature passed a bill that required entities to provide a general description of a data breach, the type of information at risk, the date and time of the breach, whether the notification was delayed because of a law enforcement investigation, and a toll-free number for major credit reporting agencies if the breach exposed Social Security numbers, driver's license numbers, or state identification card numbers.[34] This legislation was vetoed twice by then-Governor Schwarzenegger,[35] and a 2011 version of the same bill is currently before the California State Assembly.[36]

Massachusetts

Massachusetts was one of the first states to recognize the rapidly-evolving nature of modern data security and authorize a state agency to craft data security regulations.[37] Empowered by this law, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") passed regulations that require companies to develop written information security plans and to create administrative, technical, and physical safeguards to protect personal electronic data.[38] The OCABR regulations further mandate that organizations housing personal electronic data encrypt this information to protect Massachusetts residents.[39]

While the OCABR regulations have not been tested in litigation, the Massachusetts Attorney General has used these regulations as a reference point for identifying deficiencies in a business's approach to information security.[40] On March 28, the Massachusetts Superior Court approved a Final Judgment by Consent between the Commonwealth and Briar Group, LLC ("Briar"), a major restaurant group in Boston. The Commonwealth alleged that, in 2009, unauthorized individuals accessed Briar's computer network and gained customer credit card information. The Consent Judgment requires Briar to take several steps, including the implementation of a written information security program and annual reviews of its security measures; both of these Consent Judgment provisions are also requirements under the new OCABR regulations.[41]

Proposed Federal Legislation

Faced with multiple data breaches, a fractured state and federal response, and increased public scrutiny, members of Congress have proposed several different bills in 2011 which would set federal standards for consumer data protection. While Congress has considered – and failed to pass – a national data privacy law in years past, there appears to be significantly more support for such a law now. In May alone, there was a congressional hearing into the PlayStation Network breach,[42] a separate congressional hearing on consumer information in contained in smartphones,[43] and a letter from the chair of the Senate Judiciary Committee's privacy subcommittee criticizing two consumer data giants – Apple and Google – for their data privacy policies.[44] To date, the 2011 data privacy bills include the Consumer Privacy Protection Act,[45] the Commercial Privacy Bill of Rights Act,[46] and the Data Accountability and Trust Act.[47]

These bills all share common features, and at least some of these policies are likely to appear in any data protection legislation that Congress passes. Under all three bills the FTC remains the lead federal agency charged with protecting data privacy, and a violation of the proposed data privacy law is formally classified as an unfair or deceptive act or practice under the FTC Act.[48] Recognizing that inconsistent state legislation has created a "patchwork" of laws governing data privacy,[49] all three bills contain language that expressly preempts state law.[50] While these bills grant state attorneys general standing to file suit under the bills' provisions, the bills also require the attorneys general to notify the FTC of these suits.[51] If the FTC elects to file its own suit, any state attorney general proceeding is automatically stayed.[52] Finally, none of the three bills permits a private right of action.[53]

Congress' uniform focus on a top-down approach to data privacy is likely driven by two factors. First, Congress has acknowledged that there is currently only a loose network of state laws governing consumer data; since 21st century data protection is an interstate issue, Congress likely intends to set one nationwide standard to reduce confusion and streamline the logistical task of protecting consumer data. Second, because the use and scope of consumer data is changing far faster than the law, it is logical for Congress to leverage the flexibility, institutional knowledge, and discretionary enforcement of the FTC.[54]

Beyond creating a national approach to data protection, however, these bills each employ different methods to protect consumers' information. The Consumer Privacy Protection Act takes the softest approach and focuses on consumer notice and corporate self-regulation. This bill requires companies to notify consumers that personal information may be disclosed for purposes other than those for which it was collected, and that more information is available in the company's publicly-available privacy statement.[55] Under the bill, consumers can preclude the sharing of personal information with any entity that is not affiliated with the information collecting company; any such consumer preclusion remains in effect for a maximum of five years.[56] While this bill does require a company to create an information security policy and have senior management approve it, the details of that policy are left largely to the corporation itself.[57] To create a presumption of compliance with this bill, a company may submit its "self-regulation program" to the FTC.[58]

The Commercial Privacy Bill of Rights Act is the next-most rigorous bill, and it emphasizes forward-looking data protection. Under this bill, a company must create internal processes and managerial accountability to protect data,[59] provide notice to consumers of the company's data protection program,[60] and permit consumers to opt-out of the use of their personal information.[61] The bill limits the amount of information that a company can gather and requires that a company not retain this information beyond the time reasonably necessary to provide the consumer with the requested goods or services.[62] Finally, the bill creates strict requirements that a company must follow before transferring personal information to a third party.[63]

The Data Accountability and Trust Act outlines the most rigorous approach to data privacy.[64] The bill requires companies to create policies to protect consumer data, mitigate security breaches, and dispose of electronic and paper data securely.[65] For "information brokers" – entities whose primary business model is to collect or assemble information on persons who are customers of another corporation – the bill has even more rigorous provisions, including a consumer's right to review and correct erroneous information held by an information broker.[66]

Unlike the other bills, the Data Accountability and Trust Act also outlines a business' legal responsibilities after a data breach. Specifically, the bill requires a business to notify all affected customers and the FTC of the breach[67] and offer two years of credit reports and credit monitoring to affected customers.[68] However, if the data was encrypted at the time it was released and there is no reasonable risk of harm to customers, then the business is exempt from these requirements.[69] The bill also grants the FTC the authority to inform the general public of an information security breach through the FTC website.[70]

Additionally, the Obama Administration recently announced its comprehensive Cybersecurity Legislative Proposal ("Administration Proposal").[71] While the Administration Proposal covers several different areas of cybersecurity – including Internet crime, protecting critical online infrastructure, and civil liberties in cyberspace – a large portion of the Administration Proposal focuses on data breaches.[72] The Administration Proposal makes only minor changes to the breach language of the Data Accountability and Trust Act, and includes the UDAP,

preemption, and state attorneys general provisions that are present in all three bills.[73]

Conclusion

As Congress considers which bills – if any – to pass into law this session, there are three clear trends that are important for companies to follow. First, the FTC and state attorneys general will likely increase their enforcement actions when companies have data breaches. The Ceridian and Lookout complaints prove that the FTC is trying to expand the basis for a UDAP violation in this area; Congress appears likely to assist the FTC by broadening its statutory authority to secure consumer data. State legislatures are also empowering their attorneys general to pursue data breach cases, and the current legislation before Congress will continue this trend. Second, it is clear that Congress intends to simplify the regulatory burden on companies by preempting inconsistent state laws with a single federal data protection standard. Finally, both Congress and the states recognize the value in governing data privacy through regulations, rather than statutes. As data storage and threats to consumer information evolve, it is clear that Congress will follow the Massachusetts approach of empowering a regulatory agency to protect consumers. Consistent with all of these trends, companies should create their own comprehensive plans to safeguard consumer data. With increased scrutiny from the FTC, state attorneys general, and – perhaps most critically – privacy-conscious consumers, there are serious risks for companies that ignore consumer data privacy.

Elizabeth McGinn is a partner in the New York and Washington, DC offices of BuckleySandler LLP, practicing in the areas of data security, class action and complex litigation, consumer finance, fair lending, and government enforcement. Sasha Leonhardt is an associate in the Washington, DC office of BuckleySandler LLP, practicing in the areas of class action and complex litigation, government enforcement, and mortgage banking. Gastón Kuperschmit is an attorney in the Washington, DC office of Buckley-Sandler LLP, practicing in the areas of class action and complex litigation, consumer finance, and fair lending.

---

1 Eric Engleman, *Sony Faces More Questions from U.S. Lawmakers About Data Breach*, Bloomberg News, May 18, 2010, http://www.bloomberg.com/news/2011-05-17/sony-pushed-to-reveal-more-about-hacking.html.

2 Ryan Nakashima & Jordan Robertson, *Sony: Credit Data Risk in PlayStation Outage*, Forbes.com, Apr. 26, 2011, http://www.forbes.com/feeds/ap/2011/04/26/technology-specialized-consumer-services-us-sony-playstation-credit-cards-warning_8436469.html.

3 Robert McMillan, *Boeing Laptop Theft Puts U.S. Data Breach Tally Over 100M*, ComputerWorld, Dec. 15, 2006, http://www.computerworld.com/s/article/9006140/Boeing_laptop_theft_puts_U.S._data_breach_tally_over_100M.

4 Ellen Nakashima, *AOL Takes Down Site With User' Search Data*, Wash. Post, Aug. 8, 2006.

5 David Koenig, *Credit Card Data Breach Could Affect 650,000*, MSNBC.com, Jan. 17, 2008, http://www.msnbc.msn.com/id/22718442/ns/technology_and_science-security/t/credit-card-data-breach-could-affect/

6 Sharon Gaudin, *Estimates Put T.J. Maxx Security Fiasco at $4.5 Billion*, InformationWeek, May 2, 2007, http://www.informationweek.com/news/199203277.

7 Jaikumar Vijayan, *Heartland Breach Expenses Pegged at $140M – so far*, ComputerWorld, May 10, 2010, http://www.computerworld.com/s/article/9176507/Heartland_breach_expenses_pegged_at_140M_so_far.

8 *Id.*

9 Press Release, Federal Trade Commission, Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees (July 27, 2010), http://www.ftc.gov/opa/2010/07/riteaid.shtm.

10 There are, however, laws to govern data privacy in certain specific industries. *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (governing financial privacy rights with regard to financial institutions). For a detailed discussion of Gramm-Leach-Bliley please *see* Elizabeth E. McGinn & Anand S. Raman,

Consumer and Financial Services Financial Institutions and Privacy, ch. 3 (Law Journal Press 2008).

11 *See* 15 U.S.C. § 45.

12 *Id.*

13 Additionally, the FTC enforces numerous other statutes that contain privacy protections for specific sectors such as the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801-6809 (2010)), the Fair Credit Reporting Act (15 U.S.C. § 1681 (2010)), the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501-6506 (2010)), the CAN-SPAM Act (15 U.S.C. §§ 7701-7713 (2010)), and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Do Not Call Rule") (15 U.S.C. §§ 6101-6108 (2010)).

14 *See* Jay Soloway & Patricia E.M. Covington, *Data Privacy and Security: Recent Developments Affecting Consumer Finance*, 62 Bus. Law. 631, 640-42 (2007).

15 Complaint, *In re Ceridian Corp.*, No. 1023160 (F.T.C. May 3, 2011), *available at* http://www.ftc.gov/os/caselist/1023160/110503ceridiancmpt.pdf (hereinafter "Ceridian Complaint"); Complaint, *In re Lookout Servs., Inc.*, No. 1023076, (F.T.C. May 3, 2011), *available at* http://www.ftc.gov/os/caselist/1023076/110503lookoutservicescmpt.pdf (hereinafter "Lookout Complaint").

16 *See generally* Ceridian Complaint, Lookout Complaint.

17 Other consent orders the FTC has entered into for failure to provide adequate security for customers' personal information provide include: Rite Aid Corp., C-4308 (July 27, 2010) (consent order); Dave & Buster's, Inc., C-4291 (June 8, 2010) (consent order); *United States v. ChoicePoint Inc.*, No.1-06-CV-198 (N.D. Ga. Oct. 19, 2009) (stipulated final judgment); James B. Nutter & Co., C-4258 (May 5, 2009) (consent order); CVS Caremark Corp., C-4259 (Feb. 18, 2009) (consent order); Compgeeks.com, C-4252 (Feb. 5, 2009) (consent order); Premier Capital Lending, Inc., C-4241 (Nov. 6, 2008) (consent order); TJX Companies, Inc., C-4227 (Mar. 27, 2008) (consent order) and Reed Elsevier Inc., C-4226 (Mar. 27, 2008) (consent order).

18 Ceridian Complaint at 2, Lookout Complaint at 3.

19 Analysis of Proposed Consent Order to Aid Public Comment, *In re Ceridian Corp.*, No. 1023106, at 2 (F.T.C. May 3, 2011), *available at* http://www.ftc.gov/os/caselist/1023160/110503ceridiananal.pdf (hereinafter "Ceridian Analysis"); Analysis of Proposed Consent Order to Aid Public Comment, *In re Lookout Servs., Inc.*, No. 1023076, at 2 (F.T.C. May 3, 2011), *available at* http://www.ftc.gov/os/caselist/1023076/110503lookoutservicesanal.pdf .

20 Ceridian Complaint at 2.

21 Ceridian Analysis at 1 ("In particular, SQL [Structured Query Language] injection has been a well-known vulnerability for nearly a decade and is one of the most basic network vulnerabilities to address.").

22 Lookout Complaint at 2-3.

23 Agreement Containing Consent Order, *In re Ceridian Corp.*, No. 1023106 (F.T.C. May 3, 2011), *available at* http://www.ftc.gov/os/caselist/1023160/110503ceridianagree.pdf § I (hereinafter "Ceridian Consent Decree"); Agreement Containing Consent Order, *In re Lookout Servs., Inc.*, No. 1023076, at 2 (F.T.C. May 3, 2011), *available at* http://www.ftc.gov/os/caselist/1023076/110503lookoutservicesagree.pdf § I (hereinafter "Lookout Consent Decree").

24 Ceridian Consent Decree §§ II-VIII; Lookout Consent Decree §§ II-VIII.

25 Ceridian Consent Decree § II; Lookout Consent Decree § II.

26 Ceridian Consent Decree § III; Lookout Consent Decree § III.

27 Ceridian Consent Decree §§ IV-VII; Lookout Consent Decree §§ IV-VII.

28 *State Security Breach Notification Laws*, National Conference of State Legislatures, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last visited May 26, 2011).

29 *See, e.g.*, Dana J. Lesemann, *It's not the Breach, It's the Cover-Up*, 82 Fla. B.J. 20, 21 (2008).

30 Cal. Civ. Code § 1798.82(e) ("For purposes of this section, 'personal information' means an individual's first name or first initial and last name in combination with any one or more of the following data elements . . . : (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password . . . . (4) Medical information. (5) Health insurance information.").

31 Cal. Civ. Code § 1798.82(a).

32 Cal. Civ. Code § 1798.82(g)(3).

33 Cal. Civ. Code § 1798.81.5(b).

34 S.B. 20 (Ca. 2009); S.B. 1166 (Ca. 2010).

35 Cal. Franchise Tax Board, Analysis of Original Bill S.B. 24 (2010).

36 Cal. S. 24, 2011-12 Leg., (2011).

37 Mass. Gen. Laws Ann. ch. 93H. For the actual regulations *see* 201 CMR 17.01 *et seq*. For a discussion of the Massachusetts law, *see* Patricia E.M. Covington & Meghan Musselmann, Recent Privacy and Data Security Developments, 65 Bus. Law. 611, 618 (2007).

38 201 CMR 17.03.

39 201 CMR 17.04.

40 Final Judgment by Consent, Commonwealth of *Massachusetts v. Briar Group*, LLC C.A. 11-1185 Commonwealth of Massachusetts Superior Court Suffolk, *available at* http://www.securityprivacyandthelaw.com/uploads/file/Briar%20Group%20Final%20Judgment%20by%20Consent.pdf.

41 201 CMR §§ 17.03(1), 17.03(2)(i).

42 Mike Snider and Brett Molina, *Congress Blasts Sony for Response to Network Breaches*, USA Today (May 5, 2011).

43 Erica Naone, *Facebook Can't Fix Privacy Problems With Technology*, MIT Tech. Rev. (May 5, 2011), http://www.technologyreview.com/blog/editors/26779/.

44 Letter from Sen. Al Franken to Steve Jobs, CEO of Apple, Inc. and Larry Page, CEO of Google, Inc. (May 25, 2011), http://franken.senate.gov/files/letter/110525_Apple_Google_Privacy_Policy_Letter.pdf.

45 H.R. 1528 (2011).

46 S. 799 (2011).

47 H.R. 1707 (2011).

48 H.R. 1707 § 4(b); S. 799 § 402(a); H. 1528 § 10.

49 S. 799 § 2(5).

50 H.R. 1528 § 12(d); S. 799 § 405(a); H.R. 1707 § 6(a).

51 H.R. 1707 § 4(c)(3); S. 799 § 403. The only bill to not include this provision is the Consumer Privacy Protection Act, but generally state attorneys general are not permitted to sue under the FTC Act for UDAP violations, so the ability to enforce the bill remains concentrated at the federal level.

52 H.R. 1707 § 4(c)(3)(B); S. 799 § 403(c).

53 S. 799 § 406; H.R. 1528 § 11. Although H.R. 1707 does not mention a private right of action, private rights of action are not permitted for UDAP violations in other circumstances, and there is no reason to believe that the sponsors of H.R. 1707 intended to create a right of action. *See* 15 U.S.C. § 45(a)(2) ("The Commission is hereby empowered and directed . . .").

54 For a discussion of how Congress originally gave the FTC sole ability to bring UDAP actions with the understanding that the agency would use its professional discretion to create a coherent body of law, *see* Jeffrey P. Naimon & Kirk D. Jensen, *The UDAP-ification of Consumer Financial Service Law*, 128 Banking L.J. 22 (2010).

55 § 4, 5.

56 § 6 (a).

57 § 8.

58 § 9(c).

59 § 102-103.

60 § 201.

61 § 202.

62 § 301 (1-2).

63 § 302.

64 The Data Accountability and Trust Act was also introduced in 2009 as S. 2221 and 2007 as S. 495.

65 § 2(a)(2).

66 *See* § 2(b) (requiring submission of data security policies to the FTC, permitting post-breach audits, and prohibiting an information broker from using false pretenses to gain individual information); H.R. 1707 § 2(b)(3)(B).

67 H.R. 1707 § 3.

68 H.R. 1707 § 3(e)(1).

69 *Id. §* 3(f)(2)(A).

70 H.R. 1707 § 3(g).

71 Office of the President, Cybersecurity Legislative Proposal Legislative Language: Data Breach Notification, May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Data-Breach-Notification.pdf.

72 *See Id.*

73 *See Id.*