Comparison of Four Data Breach Bills Currently Before Congress (114th Session)

As of 9/10/15

A series of high profile data breaches including those of Target, Sony, Anthem, AshleyMadison.com and the federal Office of Personnel Management have created a Congressional push to establish a federal data breach standard. A number of data breach notification bills have been introduced in Congress this session and provide varying levels of protection for consumers. CDT would prefer to see strong baseline consumer privacy legislation passed that includes provisions for data breach response, as opposed to a law focusing only on breach. However, if a data-breach-specific law is passed it should give consumers equally as much if not more protection than existing federal and state laws.

Earlier this year we outlined elements that should be included in data breach legislation. These elements include: (1) an appropriately scoped preemption provision that allows states to provide its citizens with protections for data sets not covered under the federal law; (2) a broad definition of personal information so that more than just financial data is covered by the federal standard (think of the photos and videos kept in your iCloud, for example); (3) automatic consumer notification regardless of whether the breach is likely to result in a predetermined harm; (4) a requirement for companies to implement reasonable security standards and design a robust security program; and (5) enforcement authority for the FTC and state attorney generals.

The following chart compares four proposals for federal data breach legislation on the basis of these elements. Specifically, the chart compares:

- Senator Leahy's Consumer Privacy Protection Act (S. 1158). Representative Cicilline introduced a companion bill (H.R. 2977) in July.
- Senator Nelson's Data Security and Breach Notification Act (S. 177).
- Representative Blackburn's Data Security and Breach Notification Act (H.R. 1770). The House Energy and Commerce Committee approved this bill in April.
- Representative Rush's amendment in the form of a substitute to H.R. 1770. This was defeated by a roll call vote during full committee markup and it is unclear whether it will be reintroduced.

We've selected these proposals because they have received the most attention from consumer privacy advocates and provide varied approaches to data breach legislation. An extended list of data breach bills introduced in 2015 is included at the end of this chart.

Preemptive effect on existing laws

	Leahy (S.1158)	**Nelson (S. 177)**	**Blackburn (H.R. 1770)**	**Rush substitute to H.R. 1770**
Will preemption allow for states to enforce or pass laws regulating data not included in the federal bill?	Yes. Only preempts state laws that are less stringent than the requirements of the bill. (Sec. 205)	No. The preemption language is vague and creates significant uncertainty as to whether the law will preempt state laws regulating data not covered in the federal law. It preempts state law regulating "treatment of data similar to data regulated" in the bill (Sec. 7) but isn't clear on what "treatment" means.	No. Preempts any state law relating to or with respect to the security of data in electronic form or notification following a security breach of such data. (Sec. 6)	Yes. Although the preemption provision is broader than Leahy's bill, it likely would not preempt state laws that regulate data not covered in the federal law. It only preempts state laws that deal with information security practices for similar data or notification of breach. (Sec. 6)
Does the bill preempt state common law (contract, tort, etc)	No. (Sec. 205, 220)	No. (Sec. 7)	No. (Sec. 6)	No. (Sec. 6)
Does the bill preempt FCC Act provisions?	No. (Sec. 205, 220)	No.	Yes. Preempts sections 201, 202, 222, 338 and 631 of the FCC Act. (Sec. 6)	No. (Sec. 6)

Definition of personal information

	Leahy (S.1158)	Nelson (S. 177)	Blackburn (HR. 1770)	Rush substitute to HR 1770
Does it include personal photos and/or videos?	Yes. Protects "password-protected" digital photos and videos (Sec. 3)	No.	No.	Yes. Protects "user-created content" and explicitly includes photos and videos in the text. (Sec. 5)
Does it include all nonpublic communications?	No.	No.	No.	Yes. Protects all "nonpublic communications" including emails. (Sec. 5)
Does it include location data?	Yes. (Sec. 3)	No.	No.	Yes. (Sec. 5)
Does it include biometric data?	Yes. (Sec. 3)	Yes. (Sec. 6)	Yes. (Sec. 5)	Yes. (Sec. 5)
Does it include health data?	Yes. (Sec. 3)	No.	No.	Yes. (Sec. 5)
Can the FTC modify the definition?	No.	Yes. (Sec. 6)	No.	Yes. (Sec. 5)

When notification of a breach is triggered

	Leahy (S.1158)	Nelson (S. 177)	Blackburn (HR. 1770)	Rush substitute to HR 1770
Is consumer notification trigged automatically when a breach has occurred?	Yes. Must notify anyone whose information has been or is reasonably believed to have been accessed or acquired. (Sec. 211)	No. Must notify consumers *unless* entity determines there is no reasonable risk of identity theft, fraud, or other unlawful conduct. (Sec. 3)	No. Notification is only trigged *if* an entity determines there is harm. (Sec. 3)	Yes. Must notify if data was or is reasonably believed to have been acquired accessed by an unauthorized person, or used for an unauthorized purpose. (Sec. 3)

Is FTC notification triggered automatically when a breach has occurred?	No.	No. Must notify FTC *unless* the entity determines there is no reasonable risk of identity theft, fraud, or other unlawful conduct. (Sec. 3) FTC notification not required at all if entity must notify law enforcement (Sec. 4)	No.	No.
If there is a "harm trigger" is it broader than just identity theft and financial or economic harm?	There is not a "harm trigger".	Yes. Includes "other unlawful conduct". (Sec. 3)	No. Harm is "identity theft, economic loss or economic harm, or financial fraud." (Sec. 3)	There is not a "harm trigger"

Data security requirement(s)

	Leahy (S.1158)	**Nelson (S. 177)**	**Blackburn (HR. 1770)**	**Rush substitute to HR 1770**
Does the bill require covered entities to use reasonable security to protect data and put front-end security processes in place?	Yes. Requires a comprehensive data security program that includes risk assessment, management and control, as well as employee training on program. (Sec. 202). Does not mandate specific security protocols.	Yes. FTC rulemaking will outline security programs. Must require security policy, overseeing officer, vulnerability assessment and mitigation, and process for destroying data containing PII. (Sec. 2). Does not mandate specific security protocols.	No. The bill only requires entities to maintain reasonable security measures and practices (Sec. 2). No requirement that a security process be put in place. Does not mandate specific security protocols.	Yes. FTC rulemaking will outline security programs. Must require security policy, overseeing officer, vulnerability assessment and mitigation, and process for destroying data containing PII. (Sec. 2). Does not mandate specific security protocols.

Who has enforcement authority

	Leahy (S.1158)	**Nelson (S. 177)**	**Blackburn (HR. 1770)**	**Rush substitute to HR 1770**
Does the FTC have enforcement authority?	Yes. FTC can seek monetary penalties. (Sec. 203)	Yes. FTC may seek same penalties available to the agency for an "unfair or deceptive" practice under FTCA. (Sec. 5)	Yes. FTC may seek same penalties available to the agency for an "unfair or deceptive" practice under FTCA. (Sec. 4)	Yes. FTC may seek same penalties available to the agency for an "unfair or deceptive" practice under FTCA. Must coordinate with FCC and/or CFPB when enforcement affects entities subject to these agencies' authority. (Sec.4)

Do attorney generals have enforcement authority?	Yes. State and US attorney generals can seek injunction or monetary penalty. (Sec. 203)	Yes. State AGs may seek injunction, force compliance, or monetary penalties. (Sec. 5)	Yes. State AGs may seek injunction, force compliance, or monetary penalties. (Sec. 4)	Yes. State AGs may seek injunction, force compliance, or monetary penalties. (Sec. 4)
Do consumers have a private right of action?	No.	No.	No. Explicitly prohibits a private right of action. (Sec. 4)	No.
Is there a cap on penalties?	Yes. The cap is $5,000,000 unless the conduct is found to be willful or intentional.	Yes. The cap is $5,000,000 for a violation of Sec. 2 and $5,000,000 for a violation of Sec. 3	Yes. The cap is $2,500,000 for a violation of Sec. 2 and $2,500,000 for a violation of Sec. 3	No. Civil penalties are assessed by multiplying the number of days an entity is not in compliance by $11,000.

Data breach bills currently before Congress

Bill Number	**Author**
Senate	
S. 961	Sen. Tom Carper
S. 1027	Sen. Mark Kirk
S. 1158	Sen. Patrick Leahy
S. 177	Sen. Bill Nelson
House	
HR. 1770	Rep. Marsha Blackburn
HR. 2977	Rep. David Cicilline (S. 1158 companion)
HR. 1704	Rep. Jim Langevin
HR. 2205	Rep. Randy Neugebauer (S. 961 companion)
HR. 1770 amend.	Rep. Bobby Rush (amendment in the form of a substitute)
HR. 580	Rep. Bobby Rush