St. John's Law Review

Volume 92
Number 4 *Volume 92, Winter 2018, Number 4*

Article 8

Protecting Personal Data: A Model Data Security and Breach Notifications Statute

Michael Bloom

PROTECTING PERSONAL DATA: A MODEL DATA SECURITY AND BREACH NOTIFICATION STATUTE

MICHAEL BLOOM[†]

INTRODUCTION

Equifax is one of the three major consumer credit reporting agencies in the United States.[1] On July 29, 2017, Equifax discovered that hackers had breached its security and potentially compromised the sensitive information of 143 million American consumers, including Social Security numbers and driver's license numbers.[2] Hackers also gained access to names, birth dates and addresses, as well as credit card numbers for 209,000 consumers.[3] A fraud analyst stated that "[o]n a scale of 1 to 10 in terms of risk to consumers, this is a 10."[4] Another commentator stated that "[i]t is no exaggeration to suggest that a breach such as this—exposing highly sensitive personal and financial information central for identity management and access to credit—represents a real threat to the economic security of Americans."[5] This was not the first time that consumer data stored by Equifax was accessed and acquired by hackers. In 2016, hackers breached W-2 tax and salary data from an Equifax website, and in 2017, W-2 tax data from an Equifax subsidiary was stolen.[6] Identity thieves can use this stolen data to "impersonate people with lenders, creditors and service

[†] Senior Articles Editor, *St. John's Law Review*; J.D. Candidate, 2019, St. John's University School of Law; B.A., 2014, St. John's University. The Author would like to extend his gratitude to the members and editors of the *St. John's Law Review* for their dedication and immense effort throughout the publication process. He would also like to thank his family for their support and encouragement.

[1] Tara Siegel Bernard et al., *Equifax Attack Exposes Data of 143 Million*, N.Y. TIMES, Sept. 8, 2017, at A1.

[2] *Id.*; WADE BAKER ET AL., VERIZON, 2011 DATA BREACH INVESTIGATIONS REPORT 31 (2011), https://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (defining hacking as "attempts to intentionally access or harm information assets without . . . authorization by thwarting logical security mechanisms").

[3] Bernard et al., *supra* note 1.

[4] *Id.*

[5] *Id.*

[6] *Id.*

providers, who rely on personal identity information from Equifax to make financial decisions regarding potential customers."[7]

Equifax is far from being the only large corporation to have substantial amounts of its customers' sensitive information compromised. For example, in 2013, a massive hack affected three billion Yahoo accounts.[8] Yahoo did not disclose the breach to the public until September 2016, stating that data associated with at least 500 million accounts had been stolen.[9] In mid-December 2016, Yahoo disclosed a separate security breach that also dated back to 2013.[10] It was not until October 2017 that Yahoo finally disclosed that this second 2013 hack affected all three billion user accounts that existed at the time of the breach, thus "cement[ing] Yahoo's place at the top of a long and ignominious list of massive security breaches."[11]

Consumers have been plagued by other high profile data breaches, including hacks of: (1) Sony Online Entertainment consumer information of 102 million video game customers, such as names, addresses, emails, birth dates, and phone numbers of users;[12] (2) a database from Anthem, one of the nation's largest health insurers, containing eighty million records of current and former customers including names, Social Security numbers, birth dates, addresses, email and employment information, and income data;[13] (3) email addresses and account details for thirty-two million members of the site Ashley Madison, an

---

[7] *Id.*

[8] Jethro Mullen & Seth Fiegerman, *Yahoo Tops the List of Largest Ever Data Breaches*, CNN TECH (Oct. 4, 2017, 5:20 AM), http://money.cnn.com/2017/10/04/technology/yahoo-biggest-data-breaches-ever/index.html.

[9] Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN TECH (Sept. 23, 2016, 10:39 AM), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/?iid=EL.

[10] Seth Fiegerman, *Yahoo Says Data Stolen from 1 Billion Accounts*, CNN TECH (Dec. 15, 2016, 4:30 AM), http://money.cnn.com/2016/12/14/technology/yahoo-breach-billion-users/index.html?iid=EL.

[11] Mullen & Fiegerman, *supra* note 8.

[12] Charles Arthur, *Sony Suffers Second Data Breach with Theft of 25m More User Details*, THE GUARDIAN (May 3, 2011), https://www.theguardian.com/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

[13] Reed Abelson & Matthew Goldstein, *Hackers Breached Data of Millions, Insurer Says*, N.Y. TIMES, Feb. 5, 2015, at B1.

"extramarital affairs website";[14] and (4) Target, which confirmed on December 19, 2013, that credit and debit card information for about forty million customers had been stolen.[15]

The illegal acquisition of consumer information on such a wide scale can have major impacts on consumers.[16] Generally, consumers can only protect themselves from the potential consequences of these hacks if they are promptly notified that they have occurred. All fifty states require corporations to comply with certain data security standards. For example, states require that companies take certain steps to notify consumers in the event that certain types of their stored data are accessed without authorization.[17] However, there is no federal statute addressing the issue. The lack of a unified standard, as well as the absence of certain forms of protections in these state statutes, subject consumers to a greater risk of loss of their personal data's integrity than is necessary. In 2015, President Obama called on Congress in his State of the Union address to pass cybersecurity legislation because "we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information."[18] Several bills have been proposed in the last several years, including the Data Security and Breach Notification Act of 2015 (the "DSBNA" or "Act"). The bill was sent to a Senate Committee twice, but never came to a vote and was never ratified. The DSBNA sought to preempt the various state laws on data breach notification in order to create a federal standard for how and when corporations should notify consumers in the event their data was accessed. It also dictated the extent

---

[14] Robert Hackett, *What To Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/.

[15] Rachel Abrams, *Target To Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.

[16] One vulnerability expert described the Equifax breach as "a Category 5 hurricane in the cyberworld," whose "lasting impact . . . will go on for years." Andrew Soergel, *Equifax Breach Could Have 'Decades of Impact'*, U.S. NEWS & WORLD REP. (Sept. 8, 2017), https://www.usnews.com/news/articles/2017-09-08/equifax-breach-could-have-decades-of-impact-on-consumers.

[17] *Data Breach Notification Laws: Now in All 50 States,* PRIVACY RTS. CLEARINGHOUSE (May 9, 2018), https://privacyrights.org/blog/data-breach-notification-laws-now-all-50-states.

[18] Barack Obama, President of the U.S., State of the Union Address (Jan. 20, 2015). *See also* Drew Amorosi, *Obama Wants Federal Data Breach Notification Law*, DATACENTER DYNAMICS (Feb. 3, 2015), http://www.datacenterdynamics.com/content-tracks/security-risk/obama-wants-federal-data-breach-notification-law/93420.fullarticle.

of liability for failing to comply with the DSBNA's mandates. While the Act ultimately did not pass, it provides a framework, along with state notification laws, that this Note will use to set forth its arguments.

This Note argues that current law is inadequate to protect consumers in light of the prevalence and severity of data breaches in recent years, and that a unifying federal legislation combining portions of state law and the DSBNA should be enacted. Part I of this Note analyzes the DSBNA for notification requirements when data breaches occur, the requirements for the implementation of security policies, regulatory mechanisms for monitoring compliance with these requirements, and criminal penalties for failing to comply. Part II summarizes the various state laws that exist for notification of data breaches. Part III proposes a model federal statute that combines aspects of the DSBNA with current state law. Specifically, Part III argues that a preemption provision is important for creating a unified federal standard, but that provision should create exceptions for robust protections that consumers already enjoy under state law. It also argues for the inclusion of a private right of action for consumers, the removal of a reasonable risk of harm analysis, and a provision that mandates cyber risk insurance for certain covered entities.

I. THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2015

The stated purpose of the DSBNA is "to provide for nationwide notice in the event of a breach of security" and "[t]o protect consumers by requiring reasonable security policies and procedures to protect data concerning personal information."[19] The DSBNA requires the Federal Trade Commission ("FTC") to promulgate regulations requiring commercial entities to implement information security policies and procedures for the treatment of personal information.[20] It also sets out procedures that must be complied with in the event of a data breach.[21] Overall, the DSBNA goes too far in weakening consumer protection that already exists for the sake of promoting unity. This Part analyzes certain relevant provisions of the Act, addressing: (1) the definitions of personal data; (2) when and in

[19] *See generally* Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015).

[20] *Id.* § 2(a)(1).

[21] *See infra* Parts I.B and I.C.

what form notification is required to affected individuals, law enforcement, and third parties; (3) the reasonable risk of harm exemption for notification; (4) preemption; and (5) penalties for noncompliance.

A. Definitions of Important Terms in the DSBNA

The Act defines a data breach as a compromise of the security or confidentiality of electronic data that results in—or could reasonably be concluded to have resulted in—unauthorized access to or acquisition of personal information from a covered entity.[22] Covered entities include "sole proprietorship[s], partnership[s], corporation[s], trust[s], estate[s], cooperative[s], association[s], or other commercial entit[ies], and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes personal information."[23]

Personal information is defined more broadly in the DSBNA than it is in many, but not all, state statutes.[24] Under the DSBNA, personal information includes: (1) a non-truncated social security number; (2) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction; or (3) an individual's first and last name or first initial and last name in combination with (a) a driver's license number, a passport number, an alien registration number, or other similar number on a government document used to verify identity, (b) unique biometric data such as a fingerprint or voice print, (c) a unique account identifier, electronic identification number, user name, or routing code, in combination with an access code or password, (d) or any two of the following: home address or telephone number, mother's maiden name, or month, day, and year of birth.[25] This broad definition offers strong protections for consumers and triggers the notification requirements more readily than the state statutes with more restrictive definitions.[26]

---

[22] S. 177 § 6(1)(A).
[23] *Id.* § 6(3).
[24] *See* discussion *infra* Part II.A.
[25] S. 177 § 6(9).
[26] *See* discussion *infra* Part II.A.

B. Notification to Individuals and Law Enforcement

When a covered entity—an entity that owns or possesses electronic data containing personal information—discovers a breach of the security system containing that data, it must notify several individuals and entities.[27] First, the entity must notify each individual who is a citizen or resident of the United States and whose personal information is reasonably believed to have been acquired as a result of the breach.[28]

Such notification shall be made within thirty days after the date of discovery of a breach or:

> as promptly as possible if the covered entity providing notice can show that providing notice within [thirty days] is not feasible due to circumstances necessary (A) to accurately identify affected consumers; (B) to prevent further breach or unauthorized disclosures; or (C) to reasonably restore the integrity of the data system.[29]

The covered entity can provide notification in three ways: (1) in writing; (2) by email if the entity's primary means of communication with an individual is by email or if the individual has consented to receive communications by email; or (3) by any means that can be reasonably expected to reach the individual.[30]

The notification must include several points of information to comply with the requirements of the DSBNA. This includes: (1) the date of the security breach; (2) a description of the personal information that has been or is reasonably believed to have been breached; (3) a telephone number that the customer can use to contact the entity and inquire about the breach; (4) notice that the individual may be entitled to consumer credit reports under another section of the Act; (5) instructions on how to receive those credit reports; (6) a telephone number and address to contact each major credit reporting agency; and finally, (7) a telephone number and a website to obtain information regarding identity theft from the FTC.[31]

Under the DSBNA, the Secretary of Homeland Security would be required to designate a federal government entity to receive notice.[32] A covered entity would be required to notify the

---

[27] S. 177 § 3.
[28] *Id.* § 3(a)(1).
[29] *Id.* § 3(c)(1)–(2).
[30] *Id.* § 3(d)(1)(A).
[31] *Id.* § 3(d)(1)(B).
[32] *Id.* § 4(a).

designated government agency in several circumstances. First, if the number of consumers whose personal information is reasonably believed to have been acquired exceeds ten thousand.[33] Second, if the breach of security involves a database containing the personal information of more than one million individuals.[34] Third, if the breach involves databases owned by the federal government.[35] Lastly, an entity must notify the designated government agency if the breach of security involves primarily personal information of individuals known to the covered entity to be employees or contractors of the federal government involved in national security or law enforcement.[36]

The DSBNA also details what must be included in the notice to the designated federal agency. These requirements are the same as the first three requirements of notice to individuals: (1) the date of the security breach; (2) a description of the nature of the breach of security; and (3) a description of each type of information reasonably believed to have been acquired.[37] Notice must be delivered as soon as possible, but not less than three business days before notification to an individual and not later than ten days after the date of discovery of the breach.[38]

C. Reasonable Risk of Harm Exemption

Generally, an entity covered by the DSBNA is exempt from the above notification requirements if the entity "reasonably concludes" following a breach of security that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.[39] The statute in fact provides a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security if "the data is rendered unusable, unreadable, or indecipherable through a security technology or methodology," such as encryption, and this technology or methodology is generally accepted by experts in the security field.[40] This presumption can be rebutted by facts demonstrating that the security technology or methodology in a

---

[33] *Id.* § 4(b)(1).
[34] *Id.* § 4(b)(2).
[35] *Id.* § 4(b)(3).
[36] *Id.* § 4(b)(4).
[37] *Id.* § 4(c)(1).
[38] *Id.* § 4(e).
[39] *Id.* § 3(g)(1).
[40] *Id.* § 3(g)(2)(A).

specific case is reasonably likely to be compromised.[41] The Commission is to meet within one year after enactment of the Act to determine all relevant security technologies and methodologies through consultation with relevant industries and consumer organizations.[42] The Commission is then to determine which technologies and methodologies, when in use, comply with the dictates of the presumption.[43] The rules imply that entities should presume a notification requirement, unless this presumption is rebutted by a showing that there is no reasonable risk of harm to consumers.[44]

Arguably, requiring notification even when there has not been, or does not appear to be, any risk of actual harm would lead to over-notification.[45] Over-notification would increase the costs to entities by forcing them to comply with broad notification requirements, as well as by increasing the intangible costs that would be incurred through reputational damage and reduced consumer loyalty.[46] However, these potential costs will further incentivize covered entities to maintain strong cybersecurity policies and to keep up with innovations in that industry. Preferably, entities would employ policies that limit their exposure to potential breaches to the technologically possible minimum. Finding a statutory way of encouraging entities to be that thorough, proactive, and consumer-oriented in their approach is preferable to a lesser standard that merely lists some bare minimum requirements entities must comply with after a breach has already occurred.

D. Penalties and Preemption

The DSBNA does not provide a private right of action for individuals to bring suit to enforce its provisions. Instead, if the attorney general of a state "has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any covered entity who violates" the

---

[41] *Id.* § 3(g)(2)(B).

[42] *Id.* § 3(g)(3).

[43] *Id.*

[44] Patricia Bailin, *Examining the President's Proposed National Data Breach Notification Standard Against Existing Legislation*, IAPP (Feb. 27, 2015), https://iapp.org/news/a/examining-the-presidents-proposed-national-data-breach-notification-standard-against-existing-legislation/#.

[45] Jacqueline May Tom, Note, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1577–78 (2010).

[46] *Id.* at 1571.

notification requirements of the DSBNA, he may bring a civil action on behalf of the residents of that state.[47] The action may seek to enjoin further violation by the defendant, compel compliance with the DSBNA, or obtain civil penalties.[48] Damages are calculated by multiplying the days of noncompliance or the number of violations by an amount not greater than $11,000.[49] Each failure to notify a resident is considered a separate violation of the law.[50] The DSBNA caps the potential liability a defendant can face at $5,000,000 for each violation of a requirement to notify law enforcement and $5,000,000 for all violations of the requirements to notify individuals.[51]

Additionally, an attorney general can bring an action against a covered entity for violation of the requirements of notice to law enforcement agencies as well.[52] In such actions, the burden of proof is a preponderance of the evidence; once met, an entity is subject to a maximum penalty of $1,000 per individual.[53] This penalty is capped at $100,000 per day until the violation has been remedied.[54] The total amount of civil penalties that can be imposed in such a situation is $1,000,000, except where the infraction was willful or intentional.[55] In that case, an additional civil penalty of $1,000,000 can be imposed on the violating entity.[56] An attorney general can also petition a United States district court for an order enjoining an entity from engaging in any act or practice that appears to violate the notification requirements of § 4.[57]

The DSBNA also imposes liability on persons who have knowledge of a breach of security requiring notification under the Act and intentionally and willfully conceal that knowledge, if the

---

[47] S. 177, 114th Cong. § 5(d)(1) (2015).

[48] *Id.*

[49] *Id.* § 5(d)(2)(A)(i).

[50] *Id.* § 5(d)(2)(A)(ii) ("Each failure to send notification . . . to a resident of the State shall be treated as a separate violation.").

[51] *Id.* § 5(d)(2)(C).

[52] *Id.* § 5(e)(1).

[53] *Id.* § 5(e)(2)(A).

[54] *Id.*

[55] *Id.* § 5(e)(2)(B).

[56] *Id.*

[57] *Id.* § 5(e)(3).

breach "results in economic harm to any individual in the amount of $1,000 or more."[58] Such persons can be subject to a civil fine, imprisonment for up to five years, or both.[59]

The most problematic aspect of the DSBNA is that it contains a broad preemption provision. It states that no persons other than those specified above may bring a civil action under the laws of any state if such action is premised on a violation of the Act.[60] This means that private individuals cannot bring state common law causes of action for the behavior of entities that amounts to a violation of the DSBNA. The Act also supersedes "any provision of a statute, regulation, or rule of a State . . . that expressly . . . requires notification to individuals of a breach of security," with respect to covered entities under the DSBNA.[61] However, an entity is not exempt from actions sounding in common law, such as tort, under the Act.[62] As discussed below, the protections provided for in state statutes are often more consumer-oriented than protections in the DSBNA.[63] Analogous state laws requiring notification to individuals would no longer be effective if the Act was enacted as is. Enacting a federal standard with a preemption provision as broad as the one proposed in the DSBNA would have far-reaching consequences for consumers, effectively weakening their protection.[64]

II. COMPARING STATE DATA BREACH NOTIFICATION LAWS

The need for a unified federal standard and what should be included in that standard can only be determined by analyzing what protections have already been put in place by state law. As such, much like the analysis of the Act above, several categories of these laws will be examined in turn: (1) the various definitions of personal data; (2) when, in what form, and to whom notification is required; (3) the reasonable risk of harm exception; and (4) penalties for noncompliance.

---

[58] *Id.* § 1041(a).
[59] *Id.* § 1041(a).
[60] *Id.* § 7(b)(1).
[61] *Id.* § 7(a)(1).
[62] *Id.* § 7(c)(1)–(2).
[63] *See infra* Part III.A.
[64] *See infra* Part III.A.

A. *Covered Entities and Definitions of Personal Data*

Generally, under analogous state statutes, entities that conduct business in the state and that maintain computerized records of personal information are covered.[65] Most state notification statutes also require the cooperation of service providers.[66] There are some limited exceptions. For example, Minnesota's statute does not cover financial institutions, whereas the DSBNA does.[67] Additionally, Maine carves out an exception for governmental agencies that maintain records primarily for traffic safety, law enforcement, and licensing purposes.[68]

The definitions of personal data also vary across state notification statutes. For example, Colorado's recently amended statute, effective September 1, 2018, defines personal data as a "Colorado resident's first name or first initial and last name in combination with any" of the following unencrypted elements: (1) social security number; (2) student, military, or passport identification number; (3) driver's license number or identification card number; (4) medical information; (5) health insurance identification number; (6) or biometric data.[69] Colorado's definition of personal information also includes an account or credit card number in combination with any required code that would allow access to the account, or a username or email address with a password or security question answer that would allow access.[70] This definition evinces a movement to protect broader categories of personal data. Most state definitions include subsets of what is included in Colorado's amended statute. The DSBNA is less broad and does not include medical history or an individual's health insurance policy number, for example.[71] Some states do not include specific categories of data like health and medical data but do include catch-all terms like "[u]nique electronic identifier," along with the security information necessary to access the account.[72] As

---

[65] *E.g.*, ARIZ. REV. STAT. ANN. § 18-552(A) (2018); CONN. GEN. STAT. ANN. § 36a-701b(b)(1) (West 2018); MD. CODE ANN., COM. LAW. § 14-3504(b)(1) (West 2018).

[66] *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-716(2)(b) (West 2018).

[67] *See* MINN. STAT. ANN. § 325E.61(4) (West 2018) (providing an exemption to financial institutions).

[68] ME. REV. STAT. ANN. tit. 10, § 1347(3) (2017).

[69] COLO. REV. STAT. ANN. § 6-1-716(1)(g)(I)(A).

[70] *Id.* § 6-1-716(1)(g)(I)(B)–(C).

[71] S. 177, 114th Cong. § 6(9) (2015).

[72] *See, e.g.*, IOWA CODE ANN. § 715C.1(11)(a)(4) (West 2018).

our notions of what is considered personal data worthy of protection and privacy expand, that should be reflected in a unified federal statute.

B. Who, When, and How: Notification Requirements

State notification statutes vary as far as to whom they require notice be given. As you would expect, every state provides that notice must be provided to the affected individual when the notification requirement is triggered.[73] A significant portion of states require that this notice also be given to the state attorney general.[74] Further, some statutes require notice to consumer reporting agencies as well.[75]

State law varies as to how long entities have to notify the required individuals and entities. Most states require that notice be given "in the most expedient time possible and without unreasonable delay."[76] Some states provide upper limits on what is expedient and reasonable. [77]

Entities can employ several means to notify individuals of data breaches. In New York, notice can be provided in writing, electronically if the person to whom notice is being sent has consented, or via telephone.[78] If a business in New York demonstrates to the attorney general that the cost of notice would exceed $250,000, then substitute notice is available.[79] Substitute notice must consist of an email, "[c]onspicuous posting of the notice on the website page of the covered entity if the covered entity maintains one," and "[n]otification to major

---

[73] *See, e.g.*, MASS. GEN. LAWS ANN. ch. 93H, § 3(b) (West 2018); NEB. REV. STAT. ANN. § 87-803(1) (West 2018); N.Y. GEN. BUS. LAW § 899-aa(2) (McKinney 2018).

[74] *E.g.*, OR. REV. STAT. ANN. § 646A.604(1)(b) (West 2018); VT. STAT. ANN. tit. 9, § 2435(b)(3)(C)(i) (West 2018).

[75] *E.g.*, N.H. REV. STAT. ANN. § 359-C:20(VI)(a) (2018); N.C. GEN. STAT. ANN. § 75-65(f) (West 2018).

[76] CAL. CIV. CODE § 1798.82(a) (West 2018); MINN. STAT. ANN. § 325E.61(1)(a) (West 2018); *see also* MICH. COMP. LAWS ANN. § 445.72(12)(4) (West 2018) ("A person or agency shall provide any notice required under this section without unreasonable delay.").

[77] FLA. STAT. ANN. § 501.171(4)(a) (West 2018) ("Notice to individuals shall be made as expeditiously as practicable . . . but no later than 30 days."); OHIO REV. CODE ANN. § 1349.19(B)(2) (West 2018) (provides a forty-five-day time limit to provide notice); VT. STAT. ANN. tit. 9, § 2435(b)(1) (also provides a forty-five-day time limit); WASH. REV. CODE ANN. § 19.255.010(16) (West 2018) (forty-five-day time limit).

[78] N.Y. GEN. BUS. LAW § 899-aa(5)(a)–(c).

[79] *Id.* § 899-aa(5)(d). Colorado provides the same threshold cost for substitute notice availability. COLO. REV. STAT. ANN. § 6-1-716(1)(f)(IV) (West 2018).

statewide media."[80] Maine allows for substitute notice if an entity demonstrates that the cost of providing notice would exceed merely $5,000, if the affected class of individuals exceeds one thousand persons, or if the entity does not have sufficient contact information to provide written or electronic notice.[81]

Some states do not explicitly delineate what must be included in a notice given to consumers. Other states require specific pieces of information in the notice and provide guidelines on how the language of the notice should be written. For example, Washington provides that the notice of the breach must be written in plain language, and include at the minimum:

> (i) The name and contact information of the reporting person or business subject to this section; (ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and (iii) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.[82]

Virginia also provides that the notice must include "[t]he general acts of the [business] to protect the personal information from further unauthorized access [or acquisition]" and "[a]dvice that directs the [consumer] to remain vigilant by reviewing account statements and monitoring free credit reports."[83] And Colorado requires contact information for the FTC in addition to reporting agencies.[84]

C. What Triggers Notification

Similar to the DSBNA, some state laws provide that notification is not required if, after an appropriate investigation, identity theft or other fraud to any consumer is not reasonably likely to occur as a result of a breach.[85] New York's statute lists criteria that entities can consult when analyzing the risk of harm resulting from a breach, and that courts can consider when

---

[80] *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-716(1)(f)(IV).

[81] ME. REV. STAT. ANN. tit. 10, § 1347(4)(C) (2017). Kansas allows for substitute notice when the cost of providing notice will exceed $100,000 or the affected class of consumers exceeds five thousand. KAN. STAT. ANN. § 50-7a01(c)(3) (West 2018).

[82] WASH. REV. CODE ANN. § 19.255.010(14).

[83] VA. CODE ANN. § 18.2-186.6(A) (West 2018).

[84] COLO. REV. STAT. ANN. § 6-1-716(2)(a.2).

[85] MO. ANN. STAT. § 407.1500(2)(5) (West 2018); N.H. REV. STAT. ANN. § 359-C:20(I)(a) (2018); N.J. STAT. ANN. § 56:8-163(a) (West 2018).

determining if an entity's conclusion was reasonable.[86] However, some states explicitly provide that notification is required even if a covered entity determines that there is no reasonable risk of harm.[87] For example, California, the first state to enact a data breach notification statute, requires notification in the event of any unauthorized acquisition of data.[88]

D. Penalties

Finally, states are split as to whether a private right of action exists in the event of a data breach. The majority of states have decided that an individual should not have a private right of action. However, states such as Hawaii, Louisiana, and Nevada are exceptions.[89] Most states simply allow the state attorney general to bring an action on behalf of affected consumers.[90] There are very few states that provide for criminal penalties in the event of a violation of their statutes; for example, Michigan makes it a misdemeanor to notify consumers that a breach occurred when it did not.[91] Through criminal penalties, the DSBNA provides a strong incentive to comply that is absent from most state laws.

III. A HYBRID OF STATE LAW AND THE DATA SECURITY AND BREACH NOTIFICATION ACT

The diversity among the state data security laws is confusing and increases compliance costs for corporations. A unified federal standard has the potential not only to make it easier for entities to comply with statutory requirements, but also to increase consumer protection in the wake of a steady stream of cyber threats. However, the DSBNA, as written, is unable to

---

[86] N.Y. GEN. BUS. LAW § 899-aa(1)(c) (McKinney 2018) (The criteria are "(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.").

[87] CAL. CIV. CODE § 1798.82(a) (West 2018).

[88] *Id.*; *see* Tom, *supra* note 45, at 1577.

[89] HAW. REV. STAT. ANN. § 487N-3(b) (West 2018); LA. STAT. ANN. § 51:3075 (2018); NEV. REV. STAT. ANN. § 603A.270 (West 2017) (applies only to data collectors, not consumers).

[90] *E.g.*, ARIZ. REV. STAT. ANN. § 18-552(L) (2018); IDAHO CODE ANN. § 28-51-107 (West 2018).

[91] MICH. COMP. LAWS ANN. § 445.72(12)(12) (West 2018).

fulfill these goals for a variety of reasons. Instead, a model federal standard that adopts portions of both the DSBNA and current state laws would be more effective.

Five points are necessary to a successful federal statute. First, the statute must include a preemption provision that increases the strength of protections in jurisdictions with the weakest laws without diluting the protections in jurisdictions whose statutes are more consumer-oriented. Second, a federal standard must include a private right of action as a necessary remedy for individuals to assert and protect their rights, and to incentivize entities to enact strong security policies while complying with strict notification requirements. Third, entities should be required to notify individuals without unreasonable delay, as this standard allows for flexibility without posing danger to consumers from undue delay. Fourth, consumers should be notified in the event of any breach, without exceptions for a reasonable risk of harm analysis. Lastly, a federal standard should include incentives for covered entities to maintain cybersecurity insurance as both a protection for themselves as well as for consumers by extension.

A. A Model Federal Data Security and Breach Notification Statute Must Contain a Narrower Preemption Provision than the DSBNA

Even though a unified federal standard is desirable, the preemption language of the DSBNA actually weakens consumer protection for the sake of that unity. The DSBNA would preempt current state data breach notification laws in several different areas.[92] Currently, some state statutes already offer stronger data privacy protection and notification than would be provided for in the DSBNA. Those protections should not be preempted, and any federal standard should find a way to accommodate those adequate safeguards.

As a result of the diversity of data breach notification statutes across the country, many businesses that operate interstate tend to follow certain aspects of the strictest state laws

[92] Bailin, *supra* note 44 (The Act "contains a preemption provision to ensure the bill will 'supersede any provision of the law of any State, or political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data.' ").

for the sake of simplicity.[93] This means that many consumers have been protected by the requirements of the strictest state breach notification statutes in the country for certain aspects of data notification law. However, even though this has led to a partial and informal unity in an otherwise chaotic area of law, it is far less reliable than the consistent, statutorily required unity that would result from a federal statute. Further, whatever that federal standard turns out to be, if it preempts the strictest state statutes and imposes a less demanding standard, it will weaken some of the protections that consumers have enjoyed.[94]

If the DSBNA were the enacted federal standard, there are several categories of personal information protected in state statutes that would be preempted. For example, an industry has emerged around the collection and handling of consumers' health and fitness data through websites, apps, and wearable devices.[95] This type of information is not covered by the definition of personal information in the DSBNA, and any state law providing notification requirements for a breach of this category of data would no longer be in effect.[96] A few state laws even still include information in paper or other analog formats within their definitions of personal data.[97]

Some advocates have also warned that the preemption language of the DSBNA could prevent local governments from developing non-breach related data security rules.[98] It has been further suggested that, while the DSBNA itself does not propose preempting data breach regulations put in place by the Federal Communications Provision, the broad language in its preemption provision suggests that other bills that make their way to Congress might.[99] Interstate corporations trying to manage their

---

[93] G.S. Hans, *White House Data Breach Legislation Must Be Augmented To Improve Consumer Protection*, CDT (Jan. 16, 2015), https://cdt.org/blog/white-house-data-breach-legislation-must-be-augmented-to-improve-consumer-protection/.

[94] Other aspects of this Note's proposed federal standard, such as a private right of action, can only be imposed uniformly on all states if included in a federal bill. A corporation's own selfish interest to reduce compliance costs would not offer such protections.

[95] Bailin, *supra* note 44.

[96] Letter from Ctr. for Democracy & Tech. et al. to John Thune, Chairman, Senate Commerce Comm. & Bill Nelson, Ranking Member, Senate Commerce Comm. (Feb. 5, 2015) [hereinafter Letter from Ctr. for Democracy & Tech.], https://cdt.org/files/2015/02/letter-senate-commerce.pdf.

[97] *See, e.g.*, MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2018).

[98] Letter from Ctr. for Democracy & Tech., *supra* note 96.

[99] *Id.*

compliance costs need clarity on what combinations of illegally acquired data amount to a breach triggering notification. However, preempting entire categories of data that states explicitly chose to include in their legislation sacrifices the interests of consumers for the interests of large-scale sophisticated businesses. These businesses willfully assumed the responsibility of safely storing that information, and their interests should not be put ahead of the interests of consumers.

Amending the definition of personal data in the DSBNA to reflect the broadest definition in a state statute, thereby including health and medical data, analog formats, etc. would extend notification requirements and the increased protection those requirements provide. But that approach, while helpful, is not a long-term or comprehensive solution. Our perceptions of what constitutes personal data can change, as can hackers' ability to exploit pieces of information for their benefit. It would be more efficient and require less piecemeal post-hoc amending of the federal statute if it contained a modified preemption provision that does not negate the enforceability of state statutes that contain stricter provisions or broader definitions affording greater consumer protection. A preemption provision structured as such also allows states to expand protection for their constituents as technology evolves, without forcing consumers to wait for the glacially paced federal legislature to address new issues.

One possible way to structure a federal preemption statute is to ensure that it only preempts state laws that address the same areas that the federal law does. The preemption clause could also be "further narrowed to resemble the preemption standard under" a federal statutory scheme such as HITECH, "which creates a floor for data protection, rather than a ceiling."[100] Creating a floor would allow states to provide the strictest protection that their respective legislatures believe is necessary to protect their constituencies, while a unified floor would make it somewhat easier for interstate corporations to comply. Admittedly, this floor should resemble some of the highest protections currently created in state statutes. Interstate entities would likely still have to tailor their practices to the strictest protections provided for in the states in which they operate as they currently do, but only in those states. Many

[100] Hans, *supra* note 93.

intrastate entities would now be required to comply with notification requirements stricter than those they have dealt with in the past.

Unlike the DSBNA, state laws can contain specific security standards or practices that entities must comply with, whereas the DSBNA tasks the FTC with creating and promulgating those specific regulations.[101] Again, a broad preemption provision would overrule these specific state requirements and entities would only have to comply with the procedures promulgated by the FTC.[102] The effect this would have depends in large part on what the FTC decides to do. At the very least, states should be allowed to prescribe stricter procedures and policies for corporations to follow for the protection of their residents' data.

B. A Private Right of Action Should Be Included

Another necessary aspect of a model federal standard is a private right of action. Some state laws already provide for a private right of action. A federal standard that preempts these would eliminate a protection already in place for individuals in those jurisdictions.[103] After Sony's online network was breached, it faced fifty-five different class actions alleging negligence and breach of privacy.[104] Sony decided to settle at least several of these class actions.[105] This is just one example of how consumers may rely on private rights of action to protect or vindicate their interests in the event of a large-scale breach of private information. A private right of action should be available to the individuals residing in all states and territories; this can only be achieved through federal legislation.

Currently, circuit courts are split regarding what constitutes standing in a data breach lawsuit.[106] In *Pisciotta v. Old National Bancorp*, class action plaintiffs sought damages for the costs of

---

[101] Letter from Ctr. for Democracy & Tech., *supra* note 96.

[102] *Id.*

[103] *See, e.g.*, D.C. Code Ann. § 28-3853(a) (West 2018); HAW. REV. STAT. ANN. § 487N-3(b) (West 2018).

[104] Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 261 n.30 (2012).

[105] Anne Bucher, *Sony Cyberattack Class Action Settlement*, TOP CLASS ACTIONS (Feb. 26, 2016), https://topclassactions.com/lawsuit-settlements/closed-settlements/329121-sony-cyberattack-class-action-settlement/.

[106] Kevin M. LaCroix, *Deepening Circuit Split on Data Breach Suit Standing,* THE D&O DIARY (Aug. 6, 2017), http://www.dandodiary.com/2017/08/articles/cyber-liability/deepening-circuit-split-data-breach-suit-standing/.

credit-monitoring services as well as negligence for a breach of their personal information.[107] The Seventh Circuit held that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."[108] Even though the applicable Indiana law provided for a private right of action, the court determined that it was not intended for individuals to recover on such a theory.[109] However, in the D.C. Circuit, when insured persons brought a class action against a health insurer after their personal information was stolen during a data breach, the court held that the plaintiffs did indeed have standing.[110]

Some might argue that a private right of action does not need to be included in a federal standard because any preemption provisions, similar to the one proposed in the DSBNA, do not preempt common law rights of action. However, it is still unclear if individuals even have common law remedies for pursuing individual litigation due to this standing issue. Including a private right of action when entities fail to comply with notification requirements provides a remedy for individuals who face costs when their personal data is exposed. Some argue that a future risk of identity theft is not a cognizable injury and does not provide an individual the right to recover. However, that response ignores the reality consumers face and does nothing to help consumers who are exposed to greater financial risk because an entity failed to comply with notification requirements. It gives consumers two poor options. First, they can unfairly assume the costs of preemptive measures themselves. Second, they can wait until the risk of identity theft has been actualized to bring suit and suffer enduring and sometimes catastrophic consequences.

Including a private right of action would encourage entities to implement extensive cyber risk related security policies.[111] Private rights of action are "an important incentive to companies to ensure that personal data sets are protected."[112] In an action brought pursuant to a private right of action for failure to notify, "plaintiffs [would be] required to show more likely than not that

---

[107] Bonner, *supra* note 104, at 267.
[108] Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 639 (7th Cir. 2007).
[109] *Id.* at 639–40.
[110] Attias v. Carefirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017).
[111] *See infra* Part III.E.
[112] Hans, *supra* note 93.

the breach—the failure to notify—caused the plaintiff's injuries," which would "place[] an extremely heavy burden on the plaintiff."[113] Allowing individuals to bring suit simply for the failure to notify, without actual identity theft, gives persons a means to obtain the funds necessary to protect themselves from the potential future injury, a relatively small amount of money for a large corporation. In the event that an individual is actually injured, the high burden placed on the individual would limit the liability corporations face from individuals for their failure to comply.[114] Corporations would only pay large damages if their negligence truly resulted in large injuries to these individuals. This would prevent the combination of statutorily imposed penalties and individual damages awards from resulting in excessive liability for a single breach. Under the proposed standard, plaintiffs would only be able to successfully plead their case where there is sufficient evidence that an entity's non-compliance played a substantial role in the ensuing injury.

However, civil penalties in a federal data breach notification law should be uncapped. The DSBNA imposes no upper limit on how much an entity can be assessed for multiple security breaches and imposes a harsh penalty on entities that willfully or intentionally fail to comply with its requirements.[115] On the one hand, this could lead to incredibly substantial liability for corporations stemming from a single data breach. However, this additional penalty is only imposed for willful failure to comply with the notification requirements, not for the injuries sustained by individuals resulting from a breach.[116] Harsh penalties without any upper limit provide a strong incentive for covered entities to comply. As such, uncapped civil penalties, as provided for in the DSBNA, should be included in a model federal standard.

A federal standard must also make it clear that when the government collects civil penalties on behalf of his residents, the residents receive the reimbursement. If individuals are not reimbursed when an action is brought on their behalf, they either receive no remedy for the breach or are forced to bring another action for the same breach themselves. While damages provide a

---

[113] *See* Tom, *supra* note 45, at 1588.
[114] *See id.*
[115] S. 177, 114th Cong. § 5(e)(2)(B) (2015).
[116] *Id.*

strong incentive for entities to comply with the law after a breach, they do not make consumers whole again unless the funds end up in the pockets of affected individuals.

C. The Standard of Notification Without Unreasonable Delay Is the Better Standard

A federal law should provide that when notification is triggered, entities must notify individuals without unreasonable delay. The DSBNA and a minority of states require that notification be given to individuals without unreasonable delay but with an upper limit.[117] This alternative is not the best solution. Capping how long entities have to notify individuals would likely incentivize them to notify individuals quicker than they otherwise would. But, bright line rules are inflexible. A federal statute should require entities to notify individuals in the most expedient time possible and without unreasonable delay, similar to most state statutes.[118] Additionally, an upper limit may do more harm than good. There may be situations where an entity has the means to notify individuals in much less time than the commonly required thirty days. Including an upper limit on what can be considered "without undue delay" can actually give entities a "cushion to delay notification[]."[119] Some businesses argue that thirty days is too short of a window to assess the extent of and respond to a data breach.[120] In that event, when that claim is true and stands up to scrutiny from federal agencies, a more flexible window would allow entities to delay notification until it would be more proper. As long as it is objectively reasonable that the entities take that much time, it would be fairer to allow them to do so. The uncapped standard provides flexibility to deal with the exigencies of each individualized situation and is the preferable standard for a federal data breach notification law.

---

[117] *Id.* § 3(c)(1)–(2) (requiring notification be given no longer than thirty days after the discovery of a breach). *See* discussion *supra* Part II.B.

[118] *See supra* Part II.B.

[119] Bailin, *supra* note 44.

[120] Rachael King, *30 Days Not Enough Time in Obama's Proposed Breach Notification Law: Retail Group*, WALL ST. J.: CIO J. (Jan. 12, 2015, 6:00 PM), https://blogs.wsj.com/cio/2015/01/12/30-days-not-enough-time-in-obamas-proposed-breach-notification-law-retail-group/.

D. The Reasonable Risk of Harm Analysis

A federal law should not include a reasonable risk of harm exemption from notification requirements. The exemption may help corporations whose data has been breached avoid greater costs, but it ignores the rights of individuals to know when their data has been accessed. If an individual wants to preemptively take steps to avoid potential identity theft, it is vital that they know when their personal data has been accessed. "[A] consumer can only have control over his personal information if he knows who is in possession of it; therefore, increased control requires increased disclosure."[121] The idea that individuals have ownership of their personal data, even after placing it in the hands of entities, is expanding and strengthening.[122] Even if there is no substantial risk of harm, the risk an individual is subjected to after their personal data has been compromised is never fully mitigated. A person should have the opportunity to take steps to protect themselves, even if they are being overly cautious. Additionally, placing an unfettered notification requirement on covered entities provides them with still greater incentive to protect personal data above and beyond that provided by strict penalties. Entities will want to avoid the reputational harm that would result from frequent data breach disclosures. At the very least, individuals deserve to know what is happening with their data, something that ultimately belongs to them and them alone.

It should be noted that the "risk of harm analysis may keep some companies from having to undertake costly notice requirements, [but] this may not be fiscally responsible for a covered entity."[123] If a breach becomes public after an entity determines that notice is not required, "a determination that the notification requirement was not met could end up costing huge amounts of resources in litigation costs, not to mention the negative publicity that may harm business interests, irrespective

---

[121] Tom, *supra* note 45, at 1593.

[122] Greg Otto, *Why GDPR Is Flipping the Thought Process Around Data Ownership*, CYBERSCOOP (Feb. 16, 2018), https://www.cyberscoop.com/gdpr-podcast-thomas-fischer-data-security/.

[123] Kelly M. Jolley & Lindy L. Gunderson, *Data Breach Liability and Notification: What Do You Need To Know?*, S.C. LAW., Nov. 2015, at 44, 48.

of legal requirements."[124] As such, there are instances where a reasonable risk of harm analysis works against the best interests of an entity under a compliance cost analysis.

E. Cyber Risk-Related Insurance Should Be Encouraged in a Model Federal Statute

Cyber risk-related insurance would make it easier for entities whose data has been breached to compensate affected individuals. A model federal standard should include provisions that strongly encourage covered entities to maintain such policies. When Sony was hacked and the financial data for millions of consumers was stolen, Sony's potential liability was in the tens of billions of dollars.[125] Unfortunately for Sony, its insurer claimed that Sony's insurance policy did not cover cyber-related third party claims.[126] Costs resulting from a data breach can include investigating and repairing damages, notifying individuals and state agencies of the occurrence—as would be mandated by this Note's proposed standard—and managing public relations and reputational harm.[127] It is imperative that the entities covered by the proposed federal standard pursue cyber risk-related insurance policies, "which have become increasingly available over the past decade."[128]

One commentator notes that a way that the federal government can encourage companies to obtain cyber risk insurance is to mandate that government contractors and sub-contractors maintain such policies.[129] Doing so "might indirectly influence more businesses in the private industry to follow their competitors' lead."[130] Also, if a model statute included a private right of action to bring suit against entities whose data was breached, it would encourage companies to seek cyber risk insurance to protect themselves from potentially massive liability. "Cyber policies themselves impose requirements on businesses that must be met to ensure coverage, which can also help protect from a breach occurring in the first place."[131]

---

[124] *Id.*
[125] Bonner, *supra* note 104, at 261.
[126] *Id.*
[127] Jolley & Gunderson, *supra* note 123, at 44.
[128] Bonner, *supra* note 104, at 262.
[129] *Id.* at 277.
[130] *Id.*
[131] Jolley & Gunderson, *supra* note 123, at 50.

Without maintaining insurance, the costs of statutory penalties, private rights of action, and practical costs for dealing with a breach could become debilitating. This would not be beneficial for the economy or consumers. Consumers still want to use the services provided by these entities; they just want to be able to do so without subjecting themselves to a substantial risk of identity theft.

CONCLUSION

The Data Security and Breach Notification Act is comprehensive legislation that expands the scope of protection under state law in many areas. However, its broad preemption provision dilutes protections that consumers have grown accustomed to through state laws, far too extensively to be enacted as is. A model federal standard must contain a modified preemption provision that allows states the flexibility to maintain their own, more stringent standards and to adapt them as they see fit. The standard must also provide a private right of action because class actions act as an important mechanism for redressing individual wrongs, providing financial incentive to covered entities to adequately protect consumer data, and encouraging entities to enthusiastically comply with notification requirements to avoid both statutory penalties and litigation damages. There is no indication that the number of cyber attack-related data breaches is going to decrease anytime soon. The federal law proposed in this Note is the best way to create some semblance of unity in this field while increasing protection for consumers and maintaining state autonomy to legislate in this area.