COMPARATIVE ANALYSIS OF DATA BREACH LAWS: COMPREHENSION, INTERPRETATION, AND EXTERNAL SOURCES OF LEGISLATIVE TEXT

by
Carol M. Hayes[*]

Data breach laws in the United States have evolved in waves during the last couple of decades. There are a few federal laws that address aspects of data security and the aftermath of data breaches, but these laws tend to be narrow or sector-specific. This Article instead focuses on state legislative responses. As of 2018, all 50 states have a data breach law that at least addresses notifications. In this Article, the author presents the results of an empirical examination of the language used in these statutes. Examining the statutes side by side highlights the subtle choices of various state legislatures and allows for identifying distinctions that would not be clear from examining a single statute alone, including considerations of outside sources and influences on legislative text. This comparative approach to statutory interpretation is buttressed by a discussion of the dueling theories of textualism and intentionalism, the effects that the origin of statutory language should have on interpretation, and the application of lessons from social science research about language comprehension. This Article advocates for a uniform approach to data breach laws, especially as they relate to prevention, notification, and enforcement.

[*] The author worked as a Research Specialist at the Critical Infrastructure Resilience Institute. This research was supported by the Department of Homeland Security and CIRI. The author was supported by her spouse and the SCCA.

I. INTRODUCTION

Information is the building block of modern society. It drives innovations and profits. Securing that information has proven to be one of the major challenges of the 21st century. This Article is especially focused on data breaches involving the compromise of sensitive personal information. Thus far, legislative responses to data breach threats have been concentrated at the state level with no general federal data-breach legislation. The variance between state notification laws is thought by some to contribute to the high cost of responding to data breaches affecting residents of the United States. This Article presents empirical data about the variations between state laws, underscoring the need for a unified approach to data breaches. One frequently cited option for a unified approach is to enact federal data breach legislation. Conditions are right in Congress for data privacy to be a bipartisan legislative priority.[1]

[1] Diane Bartz & Sonya Hepinstall, *U.S. Senator Says Privacy Bill Draft Could Come Early Next Year*, REUTERS (Nov. 27, 2018), https://www.reuters.com/article/us-usa-ftc-congress/u-s-senator-says-privacy-bill-draft-could-come-early-next-year-idUSKCN1NX041; Dell Cameron, *U.S. Lawmakers Balk at $700 Million Equifax Fine, Renew Calls for a Federal Data Breach Law*,

This Article also explores some bigger picture issues relating to statutory interpretation, federalism, and interest groups. Data breach legislation provides a unique vehicle for this type of analysis because state laws addressing data breaches emerged in waves between about 2006 and 2018. By the end of 2018, all 50 states had enacted data breach statutes. The last two states to enact data breach laws were Alabama and South Dakota, both in 2018.[2] Such laws were crafted to address new challenges posed by technological developments and lend themselves easily to discussions about the origin of law. These laws tend to appear quite similar to each other, often with small differences that begin to seem more significant in the aggregate. Analyzing the full set of state data breach laws in existence at the end of 2018 thus enables a comparative approach to studying linguistic choice in legislation.

Individuals, companies, and service providers spent several years around the turn of the millennium learning about the convenience of storing information in a way that made it remotely accessible. Early cell phones were mostly just good for calling people, but personal digital assistants (PDAs) started to become valuable secondary devices, especially when combined with a cellular service plan. The Blackberry quickly became a status symbol in corporate America, and managers saw their personal time slowly whittled away as their work email started arriving on these devices that they kept in their pockets or purses. Productivity time expanded to include commutes and weekends. Many companies adopted Bring Your Own Device (BYOD) policies to encourage this increased productivity without the increased cost of providing everyone with new devices.[3]

Work email in your pocket was just the beginning. Broad adoption of internet technology fueled the rise of telecommuting, and employees were able to take their work home and still have access to important files at the office. The CEOs benefited, but so did data thieves. Trade secrets and customer information were now held on networks that could potentially be compromised by a simple phishing attack, and with the rise of telecommuting, these networks were becoming more accessible. Identity theft became a pervasive threat thanks to data insecurity affecting confidential personal information like social security numbers and payment data.

The convenience of interconnectedness led to other downsides as well. In 2015, users of the adultery-facilitating website Ashley Madison were humiliated when a

GIZMODO (July 23, 2019), https://gizmodo.com/u-s-lawmakers-balk-at-700-million-equifax-fine-renew-1836640703.

[2] Bailey Langner, *South Dakota and Alabama Last Two States to Enact Data Breach Law*, JD SUPRA (Apr. 11, 2018), https://www.jdsupra.com/legalnews/south-dakota-and-alabama-last-two-24878/.

[3] *See* IBM, *Bring Your Own Device*, https://www.ibm.com/mobile/bring-your-own-device (last visited Oct. 25, 2019).

public posting of the website's user database unmasked their names.[4] During the 2016 presidential race in the United States, a large number of allegedly state-sponsored cyberattacks targeted political organizations and state voter databases.[5] Thousands of medical appointments were disrupted in May of 2017 when the WannaCry ransomware attack locked medical professionals out of computer systems that operated as part of the United Kingdom's National Health Service.[6] In September 2017, the American public was informed that Equifax, one of the country's "big three" credit report bureaus, had experienced a massive data breach affecting 148 million consumer records.[7]

The United States Congress has occasionally enacted legislation about cybersecurity, but progress has been slow. In 2013, President Obama signed Executive Order (EO) 13,636, which addressed critical infrastructure cybersecurity and tasked the National Institute of Standards and Technology (NIST) with the responsibility of developing the Cybersecurity Framework for use by critical infrastructure providers.[8] In 2014, Congress passed three cybersecurity-related bills: 1) the Federal Information Security Modernization Act of 2014 (FISMA);[9] 2) the National Cybersecurity Protection Act of 2014 (NCPA);[10] and 3) the Cybersecurity Enhancement Act of 2014 (CEA).[11] FISMA is an update to the Federal Information Security Management Act.[12] The NCPA codifies the functions of the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS).[13] Title I of the CEA includes guidelines for NIST's activities relat-

[4] *See* Julia Greenberg, *Private Investigator Startup Exploits Ashley Madison Hack*, WIRED (Aug. 25, 2015), https://www.wired.com/2015/08/private-investigator-startup-exploits-ashley-madison-hack/.

[5] Cynthia McFadden et al., *U.S. Intel: Russia Compromised Seven States Prior to 2016 Election*, NBC NEWS (Feb. 27, 2018), https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296.

[6] *NHS "Could Have Prevented" WannaCry Ransomware Attack*, BBC NEWS (Oct. 27, 2017), https://www.bbc.com/news/technology-41753022.

[7] Alyza Sebenius & Jennifer Surane, *Equifax Failed to Match Security to Its Growth, Report Says*, BLOOMBERG (Dec. 10, 2018), https://www.bloomberg.com/news/articles/2018-12-10/equifax-failed-to-adjust-security-to-rapid-growth-report-says.

[8] Exec. Order No. 13,636, 78 Fed. Reg. 11,740–41 (Feb. 12, 2013).

[9] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (codified in scattered sections of the United States Code).

[10] National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (codified in scattered sections of the United States Code).

[11] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 129 Stat. 2971 (codified in scattered sections of the United States Code).

[12] Federal Information Security Modernization Act, 44 U.S.C § 3551 (2012); Federal Information Security Management Act of 2002, *id.* §§ 3551–3559.

[13] National Cybersecurity Protection Act of 2014, 6 U.S.C. § 148 (2012).

ing to cybersecurity standards, codifying certain aspects of EO 13,636. NIST's Cybersecurity Framework has since become a resource for cybersecurity standards outside of critical infrastructure as well.

Some federal cybersecurity laws focus on the need for cyber-threat information to be shared between the private sector and the government. In 2015, Congress enacted the Cybersecurity Information Sharing Act (CISA) as part of the 2016 omnibus spending bill.[14]

On the consumer protection side, the 2017 Equifax breach prompted Congress to finally address credit freezes, a tool available to consumers after a data breach. When a consumer requests a credit freeze, the credit bureau puts a block on new credit requests from lenders.[15] This prevents identity thieves from using the consumer's information to open a new account. When the consumer wants to apply for credit again, the consumer can unfreeze his or her credit report. Until September 2018, state law regulated credit freezes,[16] and credit agencies could charge consumers a fee for the freezing service.[17] Often, the credit agencies charged separate fees to freeze and unfreeze the individual's credit.[18] With the new federal law, the three major credit bureaus must provide credit freezes at no charge.[19]

Carl Sagan said that before you can bake an apple pie from scratch, you must first create the universe.[20] This Article does not seek to create a data breach law from scratch, but does seek to understand the universe that shaped the current state of data breach law. The first path of this analysis examines statutory interpretation and language comprehension. The quantitative and qualitative study of legislative language is built on assumptions, and this Article explores some of these assumptions that are relevant to how lawyers read, comprehend, and interpret legislative text.

Statutory interpretation can be approached from a reader-centric perspective or from a writer-centric perspective.[21] The former asks how a reasonable reader would interpret a passage, and the latter asks how a reasonable legislator intended

---

[14] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 129 Stat. 2936 (2015) (codified in scattered sections of the United States Code).

[15] Janna Herron & Adam Shell, *Freezing Your Credit Is Free in All States Under a New Law Following Equifax Breach*, USA TODAY (Oct. 5, 2018), https://www.usatoday.com/story/money/2018/09/21/equifax-free-credit-freeze-new-law/1377815002/.

[16] *E.g.*, CAL. CIV. CODE § 1785.11.2 (West 2019).

[17] Ann Carrns, *New Law Will Let Consumers "Freeze" Credit Files Without Charge*, N.Y. TIMES (June 1, 2018), https://www.nytimes.com/2018/06/01/your-money/credit-freeze-new-law.html.

[18] Katie Lobosco, *Congress Just Made Credit Freezes Free*, CNN (May 22, 2018), https://money.cnn.com/2018/05/22/pf/free-credit-freeze/index.html.

[19] 40 U.S.C. § 102 (2012).

[20] *Cosmos: The Lives of the Stars* (PBS television broadcast Nov. 23, 1980).

[21] Morell E. Mullins, Sr., *Tools, Not Rules: The Heuristic Nature of Statutory Interpretation*, 30 J. LEGIS. 1, 20 (2003).

the passage. This Article applies a writer-centric perspective and to this end also explores policy issues relating to statutory language that originated outside of legislatures or legislative drafting offices. This leads to the second path of analysis about the structure of government, law, and power.

This second path explores some foundational topics relating to law and governance. An overarching purpose of governance is to provide balance between groups with conflicting interests. The pig farmer wants to expand operations, but the new neighbors don't want the smell. It is a basic 1L discussion topic, pitting the right to have nice smelling air against the right to make a living. A neutral arbiter can listen to both sides and decide whether the solution should favor the neighbors or the farmer. The outcome will depend on deep-seated social values about individual choices and group cohesion. Is the social value of the pig farmer's activity greater than the neighbors' interest in clean air? Is the increased harm to group welfare from the foul odors greater than the marginal benefit to the farmer from expansion?

The interaction between conflicting values is further explored in the context of political pressure on legislation, such as by lobbyists and similar organizations. The content of state data breach laws depends on the balance of equities between the interests of the data subjects and the interests of the data holders. The transfer of data to third parties has traits of contract and property. It is generally assumed that data subjects receive something in exchange for their data, like a frequent shopper discount at a grocery store. The frequent shopper example is a contract model of data exchange. But data transfers also have a quasi-property element to them that is tied to what Samuel Warren and Justice Louis Brandeis might have called a right of "inviolate personality."[22]

Is there actually a right of inviolate personality in shopping habits, though? Consider a recent morality tale about big data and shopping habits involving the retail chain Target.[23] A father goes to the local Target, upset because his teenage daughter has been receiving coupons in the mail for baby clothes and cribs. The manager apologizes profusely and promises to follow up on the matter. A few days later, the manager calls the father again, though this time the father is more sheepish about the topic. It turned out that his daughter was actually pregnant, and Target figured this out before she had a chance to tell him, thanks to an alignment of statistics, unscented lotion, cotton balls, and multivitamins. As this example shows, patterns of consumption can reveal a great deal about an individual's personal life, thus potentially implicating the right of inviolate personality invoked in *The Right to Privacy*.

---

[22] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890); *see also* David Rosen & Aaron Santesso, *Inviolate Personality and the Literary Roots of the Right to Privacy*, 23 LAW & LITERATURE 1, 4 (2011).

[23] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Privacy theory has evolved with technology, perhaps in response to how new possible uses of technology create some amorphous sense of discomfort. Andrew Pole, who created Target's pregnancy-prediction model based on guest purchases, acknowledged that perfectly legal uses of data might nonetheless cause people to "get queasy."[24] Privacy law may then evolve to address this sense of unease, which this Article anoints "the squick factor."

The third part of this Article provides empirical analyses of each state data breach law. By analyzing data breach laws relative to each other, this Article adopts a comparative approach to statutory interpretation. This kind of comparative statutory interpretation is built on the bones of federalism. By examining the small differences in how states address data breaches in their codes, this Article attempts to draw out meaningful conclusions about how data breach issues are prioritized nationally.

This Article makes three primary recommendations. First, a unified data breach law should address prevention, and the NIST Cybersecurity Framework is a potentially useful tool for this end. Second, a unified data breach law must address notifications, and this Article recommends a reasonableness standard that includes law enforcement investigations, private breach investigations, and system restoration. Third, a unified data breach law must have an enforcement goal. This Article builds on past work in the area by calling for a data breach compensation fund that could be used for digital cleanup costs and individual compensation.

II. INTERPRETING AND COMPREHENDING LEGISLATION

Any legal analysis implicitly draws from theories about the origins and legitimacy of the very concept of law. The preeminent jurist Oliver Wendell Holmes promoted a predictive theory of law.[25] Justice Holmes, widely considered the founder of the legal realism movement, believed that the law was more appropriately understood as a set of predictions of how courts will act.[26] Law can also broadly be viewed as a tool for advancing the norms of social welfare and democratic legitimacy.[27]

The role of judges is to apply the language of statutes and other rules to real world situations. This requires a constant balance between consistency and correction. Karl Llewellyn noted that courts looking at the same novel situation might say

---

[24] *Id.*

[25] *See* O. W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 457 (1897).

[26] *See* David V. Snyder, *Private Lawmaking*, 64 OHIO ST. L.J. 371, 373 (2003); Catharine Pierce Wells, *Holmes on Legal Method: The Predictive Theory of Law as an Instance of Scientific Method*, 18 S. ILL. U. L.J. 329, 329 (1994).

[27] Abbe R. Gluck et al., *Unorthodox Lawmaking, Unorthodox Rulemaking*, 115 COLUM. L. REV. 1789, 1836 (2015).

something like: "that rule is too well settled in this jurisdiction to be disturbed" and apply it; or, "that rule has never been extended to a case like the present" and then not apply it.[28] That decision creates a precedent, giving that interpretation *stare decisis* effect. Consistency is at the core of the application of law.

Other approaches to law encourage correction and evolution. Dissenting in *Burnet v. Coronado Oil & Gas Co.*, Justice Brandeis acknowledged that "in most matters it is more important that the applicable rule of law be settled than that it be settled right."[29] Still, Justice Brandeis advocated for more flexibility in overruling past precedent on questions of constitutional law, reasoning that the process of trial and error is valuable in law just as it is in the sciences.[30] Llewellyn took a similar approach when he asserted that by applying or overturning precedent, courts constantly work towards improving the law.[31]

The application of the law depends on choices made by fallible judges. Robert Martineau criticizes the view that statutory interpretation is based on some grand theory and argues instead that a court's opinion is best understood as a reasoned justification for the decision.[32] It is of little wonder that there are so many legal policy debates between realists who view law as prediction and opinions as justification.

This Section explores the law as language. The following Section explores the law as institution. Law is shaped by power dynamics and balancing responsibilities. The government cedes power to citizens to form private agreements and retains the power to enforce those agreements.[33] Political scientist and philosopher Arthur Bentley said that law "is government . . . stated from a different angle."[34] Dissertations can be written on these subjects, but the emphasis of this Article is to understand data breach responses through the lenses of both law as language and law as institution.

A. Statutory Interpretation

Viewing law as language, communication is key. Scholars may distinguish between interpretation and construction of law. Aaron Tang describes interpretation as an empirical act focused on the text and construction as a normative act that

---

[28] Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are to Be Construed*, 3 VAND. L. REV. 395, 395 (1950).

[29] Burnet v. Coronado Oil & Gas Co., 285 U.S. 393, 406 (1932) (Brandeis, J., dissenting).

[30] *Id.* at 406–08 (Brandeis, J., dissenting).

[31] Llewellyn, *supra* note 28, at 399.

[32] Robert J. Martineau, *Craft and Technique, Not Canons and Grand Theories: A Neo-Realist View of Statutory Construction*, 62 GEO. WASH. L. REV. 1, 27 (1993).

[33] Snyder, *supra* note 26, at 414. In describing the patterns of private lawmaking, Snyder notes that contracts can undermine statutory language. *Id.* at 412.

[34] ARTHUR F. BENTLEY, THE PROCESS OF GOVERNMENT 272 (1908).

identifies the text's legal effect.[35] By this standard, this Article focuses primarily on statutory interpretation. A comparative approach to data breach laws enables examination of the negative space, and these negative spaces provide the contours of policy debates. The application of text to specific situations is beyond the scope of this Article.

The most basic source for statutory interpretation is the text of the statute. When faced with textual ambiguity, courts often turn to canons of construction to determine how various aspects of the text affect a statute's meaning.[36] Judge Richard Posner describes meaning as "what emerges when linguistic and cultural understandings and experiences are brought to bear on the text."[37] Often left unspoken is the assumption that interpretations must be objective and not affected by a desire to achieve a particular outcome. Maureen Cavanaugh argued that principled interpretation is necessary to the rule of law.[38]

In *Smith v. United States*, the Supreme Court held that trading a gun for drugs counts as the use of a firearm in relation to a drug-trafficking crime under federal law.[39] Both "use" and "in relation to" could be read ambiguously. The majority pointed to another provision of the same statute where "use" seemingly encompassed the trade of firearms,[40] and noted that "in relation to" was an expansive phrase.[41] Thus, trading a gun for drugs counted as a "use" under the statute. In his dissent, Justice Scalia criticized the majority's interpretation of "use" as going against the ordinary meaning of the word in the context of a statute about firearms.[42] Justice Scalia asserted that the ordinary meaning of using a firearm was that it was used "as a weapon."[43]

The various nuances of language complicate statutory interpretation, so understanding context is often critically important.[44] Consider homonyms, which are words that are spelled the same but have different meanings. Homonyms have been discussed in the statutory interpretation context for centuries. William Blackstone cited an example of a law that prohibited "ecclesiastical persons" from purchasing

---

[35] Aaron Tang, *Reverse Political Process Theory*, 70 VAND. L. REV. 1427, 1465 (2017).

[36] *See* Llewellyn, *supra* note 28, at 401 (asserting that each canon has an opposite canon).

[37] RICHARD A. POSNER, THE PROBLEMS OF JURISPRUDENCE 296 (1990).

[38] Maureen B. Cavanaugh, *Order in Multiplicity: Aristotle on Text, Context, and the Rule of Law*, 79 N.C. L. REV. 577, 659 (2001).

[39] Smith v. United States, 508 U.S. 223, 237 (1993).

[40] *Id.* at 234–35.

[41] *Id.* at 237.

[42] *Id.* at 242 (Scalia, J., dissenting).

[43] *Id.*

[44] Jill C. Anderson, *Misreading Like a Lawyer: Cognitive Bias in Statutory Interpretation*, 127 HARV. L. REV. 1521, 1534 (2014).

"provisions" in Rome.[45] The more common interpretation of provisions as personal goods fits oddly there, but the statute makes more sense when you know that "provision" has a separate meaning in Catholicism, referring to a category of papal nominations.[46] "Provision" here is a homonym, but the two meanings are distinct enough that context will often provide clarity.

Statutory interpretation principles can have some influence on legislation and regulations. State drafting offices keep drafting manuals to guide aspects of the drafting process.[47] Many manuals warn of specific ambiguity hazards, like misplaced modifiers, the choice between "shall" and "may," and the choice between "that" and "which."[48] These drafting manuals often include guidance about statutory interpretation principles, and courts are increasingly looking to these drafting manuals for interpretive clues, creating an active dialogue between legislatures and courts.[49]

A study of the federal legislative process showed that the drafters of congressional legislation often do not consider statutory interpretation principles.[50] Depending on how effectively the instructions are followed in the states, this could suggest that there is more of a feedback loop between state legislatures and state courts than there is between Congress and federal courts. At the federal level, a more visible feedback loop exists between Congress and executive agencies.[51] Agencies, for example, often refer to legislative history when drafting rules, and they are involved in the legislative drafting process to varying degrees.[52]

Statutory interpretation has been complicated in recent years by the rise of unorthodox lawmaking practices like the use of omnibus and emergency bills.[53] For example, the Authorization for the Use of Military Force (AUMF) was enacted on

---

[45] 1 WILLIAM BLACKSTONE, COMMENTARIES *60.

[46] *Id.*

[47] Grace E. Hart, *State Legislative Drafting Manuals and Statutory Interpretation*, 126 YALE L.J. 438, 443 (2016).

[48] *Id.* at 465–66.

[49] *Id.* at 442, 487. Hart notes that courts generally use drafting manuals for two purposes: determining the meaning of particular words or phrases and providing insight into the context of the legislative history. *Id.* at 479; *see also* Gary L. Anderson & Liliana Montoro Donchik, *Privatizing Schooling and Policy Making: The American Legislative Exchange Council and New Political and Discursive Strategies of Education Governance*, 30 EDUC. POL'Y 322, 334 (2016) ("According to discourse analysts, all texts are dialogical, meaning that they are in dialogue with other texts, whether explicit or implicit.").

[50] Abbe R. Gluck & Lisa Schultz Bressman, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part I*, 65 STAN. L. REV. 901, 907 (2013).

[51] *See* Christopher J. Walker, *Legislating in the Shadows*, 165 U. PA. L. REV. 1377, 1405 (2017). Walker suggests that the involvement of federal agencies in the legislative process supports viewing agency interpretations of statutes through a "purposivist" lens. *Id.*

[52] *See id.* at 1400.

[53] Gluck et al., *supra* note 27, at 1803.

September 14, 2001, and has served as the foundation of subsequent counterterrorism policies.[54] Some question whether imbuing the AUMF with this kind of authority is excessive given the unique and sensitive circumstances of its enactment.[55] Another example is omnibus bills, which used to be an extreme remedy but now effectuate an increasing number of important policy changes. An example of this in the federal cybersecurity context is the Cybersecurity Information Sharing Act (CISA), an important piece of legislation about sharing cyber threat information between the public and private sectors.[56]

1. Dueling Theories

There are a variety of approaches that courts may take to resolve ambiguities and uncover meaning. Broadly, textualism is associated with an emphasis on the plain or ordinary meaning of the language, and intentionalism is associated with an emphasis on legislative intent.[57] Generally speaking, textualism and intentionalism operate in line with each other until a law's purpose conflicts with its literal text.[58] A third major option is dynamic interpretation, which starts with the text and then addresses concerns relating to when the law was enacted and whether things have changed in ways the original legislature did not anticipate.[59]

A textualist analysis will often emphasize the "ordinary reader" and can thus be described as a reader-centric model.[60] Intentionalism examines the intent of the legislature and can thus be described as a writer-centric model.[61] Dynamic interpretation is a more flexible approach that applies elements of textualism and intentionalism.[62] One criticism of dynamic interpretation is that there is not a single unified theory,[63] but this may also be one of its strengths.

Statutory interpretation uses a variety of tools, often depending on which theory is being applied. An intentionalist interpreter might ask what the legislators intended, use legislative materials to discern intent, or ask themselves how a reasonable legislator would respond to a particular interpretive question.[64] Textualists often reject legislative history in favor of relying on the plain or ordinary meaning of the

---

[54] *Id.* at 1808.

[55] *Id.*

[56] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 129 Stat. 2936 (2015) (codified in scattered sections of the United States Code).

[57] Cavanaugh, *supra* note 38, at 582.

[58] Anderson, *supra* note 44, at 1536–37.

[59] Cavanaugh, *supra* note 38, at 598.

[60] Mullins, *supra* note 21, at 24–25.

[61] *Id.*

[62] Cavanaugh, *supra* note 38, at 582.

[63] *Id.* at 599–600.

[64] Mullins, *supra* note 21, at 25.

words.[65] To get at the plain meaning, textualists often consult extra-statutory sources like dictionaries, which critics point out are hardly part of the statute.[66]

Both intentionalism and textualism have structural flaws. Critics of using legislative history as an interpretive tool warn that such a tool can be misused or have misleading implications.[67] Others point out that a legislative entity cannot have an intent the same way as an individual has intent.[68] Rigid textualism, on the other hand, may overlap with the kind of formalism where power is determined by who can best manipulate the rules in their favor.[69]

2. Interpretation and Statutory Organization

In analyzing data breach statutes, one factor to consider is how the statute is organized. Placing a data breach statute in a consumer protection area of the code communicates a slightly different legislative priority than placing the statute in a chapter about computer security. Structure is sometimes discussed as an element to consider during interpretation.[70] With some elements of structure, like section headings, there are disagreements about the extent to which these elements should affect construction.[71]

It is possible that a comparative structural approach to interpretation is only viable in limited circumstances. The structure of tax law, for instance, is one that scholars have emphasized.[72] Data breach statutes present a valuable opportunity for analyzing statutes, including their structure, comparatively.

B. Language and Comprehension

The previous subsection discussed statutory interpretation because such theories are essential to understanding how language is used by lawyers and judges. This subsection expands that inquiry to the use of language in general, including issues relating to linguistics and language comprehension. Holmes wrote that "certainty

---

[65] Cavanaugh, *supra* note 38, at 595–96.

[66] *Id.* at 597–98.

[67] *Id.* at 589–90.

[68] Mullins, *supra* note 21, at 10.

[69] Cavanaugh, *supra* note 38, at 620.

[70] *Id.* at 611; Michael Livingston, *Congress, the Courts, and the Code: Legislative History and the Interpretation of Tax Statutes*, 69 TEX. L. REV. 819, 832 (1991).

[71] Hart, *supra* note 47, at 459 (discussing legislative drafting manuals' handling of headings for interpretation).

[72] *See, e.g.*, Deborah A. Geier, *Interpreting Tax Legislation: The Role of Purpose*, 2 FLA. TAX REV. 492, 497 (1995) ("But the fundamental structure of the income tax . . . is a larger constraint, a larger purpose, that must inform interpretation of those provisions that implicate it."); Lawrence Zelenak, *Thinking About Nonliteral Interpretations of the Internal Revenue Code*, 64 N.C. L. REV. 623, 657 (1986) (discussing the adoption of nonliteral interpretations based on structure and policies).

generally is illusion."[73] Language is imprecise by nature, and lawyers can spend whole careers trying to force words into a place of precision.[74] This emphasis on precision in language may make it harder for clients to understand their own cases.[75] The ongoing quest for balance between precision and readability in the law is further complicated by two considerations: how language is comprehended and how language is structured.

1. Legal Language and Cognitive Science

Written language is fundamentally just marks on paper, and the brain frequently makes inferences beyond the text itself to arrive at the text's meaning.[76] Statutory text is usually written at a high level of generalization, creating many opportunities for presuppositions to shape interpretations.[77] Psychological studies have shown that new information is often interpreted to be consistent with preexisting beliefs.[78] In other words, the problem is not just ambiguous homonyms, but how we as humans actually process our environment.

When making decisions, people often consciously or unconsciously employ general rules of thumb, or heuristics. The representativeness heuristic, for example, is based on the assumption that things with similar behaviors are similar.[79] The availability heuristic is another shortcut that describes a person's tendency to form conclusions based on information to which they are regularly exposed.[80] In many cases, the use of heuristics leads to reasonable outcomes.

Dual process theories of cognition posit that there is a fast cognition path that is intuitive and associative, and a slow cognition path that is analytical and algorithmic.[81] Fast cognition is especially susceptible to cognitive bias because of its reliance on heuristics.[82] Cognitive biases appear in many forms. One study found that a hypothetical DUI defendant was more likely to be judged as guilty by study participants when the defendant was described as being a member of a college fraternity.[83]

---

[73] Holmes, *supra* note 25, at 466.

[74] *See* Mullins, *supra* note 21, at 45–46 (noting that "[w]ords are approximations").

[75] Edith Greene et al., *Do People Comprehend Legal Language in Wills?*, 26 APPLIED COGNITIVE PSYCH. 500, 501 (2012).

[76] Mullins, *supra* note 21, at 41.

[77] *Id.* at 42.

[78] Barak Orbach, *Invisible Lawmaking*, 79 U. CHI. L. REV. DIALOGUE 1, 12–13 (2012).

[79] Mullins, *supra* note 21, at 51.

[80] Allison Kramer & Michele Van Volkom, *The Influence of Cognitive Heuristics and Stereotypes About Greek Organizations on Jury Decisions*, 23 PSI CHI J. PSYCH. RES. 51, 52 (2018); Kendra Cherry, *How the Availability Heuristic Affects Decision Making*, VERY WELL MIND (May 18, 2019), https://www.verywellmind.com/availability-heuristic-2794824.

[81] Anderson, *supra* note 44, at 1574.

[82] *Id.* at 1575.

[83] Kramer & Van Volkom, *supra* note 80, at 57.

Addressing cognitive bias in the courtroom thus may require awareness of how mental shortcuts function and how to offset incorrect shortcuts.

Like cognition generally, text comprehension is also subject to varying layers of processing. One theory of text comprehension is that there are three levels: a surface level representation, a representation based on lexical and syntactical meaning, and a situational representation.[84] Researchers have found that simplifying legal language, such as that found in jury instructions, informed consent forms, and wills, can increase comprehension of the legal provisions by laypersons.[85]

One factor that complicates statutory interpretation is that statutes are written in the legislative context and then applied in the context of the judicial process.[86] Legal documents are also typically written at a high reading level. Australia and New Zealand have used readability statistics to work on improving their tax codes.[87] One research team found that enhancing understanding of legal text required syntactic simplification and lexical clarification.[88] Comprehension, then, is related to and benefits from linguistic choices and structure.

2. Law and Psycholinguistics

Writing is central to the legal profession, but the study of language is often taken for granted when analyzing statutes. This Article considers cognitive processing as it relates to the act of analyzing statutory language. This research highlights the potential for interdisciplinary academic examinations of cognition, language processing, and statutory interpretation.

Jill Anderson's compelling recent article on cognitive bias is an example. She notes that legal ambiguity can often be traced to the use of opaque verbs in statutes.[89] Opaque verbs contrast with transparent verbs, which describe more concrete interactions between the subject and object of a sentence. Opaque verbs often apply to mental states. Anderson emphasizes that sentences using opaque verbs often lend themselves to both *de re* and *de dicto* interpretations.[90] A *de re* interpretation of a sentence focuses on the object as a thing, while a *de dicto* interpretation focuses on the object as a representative of a category.[91] Some cognitive development research

---

[84] Greene et al., *supra* note 75, at 501.

[85] *See id.* at 502–04. In its study of wills, Greene's research team basically provided participants with a mini-law school exam for non-lawyers, and part of that mini-exam centered on the rule against perpetuities. *Id.* at 502.

[86] Mullins, *supra* note 21, at 34.

[87] Greene et al., *supra* note 75, at 502.

[88] *Id.* at 506.

[89] Anderson, *supra* note 44, at 1532.

[90] *Id.* at 1533.

[91] *Id.* at 1532–33.

suggests that *de re* interpretations of language occur earlier in development than *de dicto* interpretations.[92]

To illustrate opacity, Anderson uses the example: "I am looking for a piece of paper."[93] It is unclear if the speaker is looking for a specific piece of paper (the *de re* interpretation) or if any sample of paper will do (the *de dicto* interpretation). There is, in other words, an ambiguous relationship between the subject of the sentence, "I," and the object of the sentence, a piece of paper. The sentence, "I am writing on a piece of paper," is transparent. There is a specific piece of paper, and the relationship between the subject and object is clear.

A similar structure is at play in federal obstruction of justice statutes. Under 18 U.S.C. § 1503, it is a federal offense to endeavor to obstruct the administration of justice.[94] Anderson notes that this was historically interpreted to require the existence of a specific investigation, which is the *de re* interpretation of the clause.[95] This interpretation can be traced back to *Pettibone v. United States*, where unionized miners on strike were charged with obstruction because of interference with mining operations.[96] This was because a federal court had issued an injunction against interfering with the mine. By striking, the miners were thus violating a court order, an arrangement which seems to be a relative of *ex post facto* laws. Instead of being discussed in those terms, however, the court dismissed the obstruction case based on the miners' lack of intent to interfere with a specific court order.

Over a century later, the principles of *Pettibone* were applied to protect Arthur Andersen, Enron's accounting firm, in *Arthur Andersen LLP v. United States*. When the Enron scandal surfaced, Arthur Andersen started shredding documents in anticipation of litigation, and stopped doing so when the SEC served it with a subpoena.[97] This situation was an inverse of the situation in *Pettibone*—there, a court order at least existed at the time of the disruption. Because the shredding was not in response to a court order, the Court found that there was no obstruction.[98] Federal obstruction law was subsequently amended to address this perceived failure to hold Arthur Andersen accountable.[99]

---

[92] *Id.* at 1569–70.

[93] *Id.* at 1532.

[94] 18 U.S.C. § 1503(a) (2012).

[95] Anderson, *supra* note 44, at 1546–47.

[96] Pettibone v. United States, 148 U.S. 197, 206 (1893) ("[A] person is not sufficiently charged with obstructing or impeding the due administration of justice in a court unless it appears that he knew or had notice that justice was being administered in such court."); Anderson, *supra* note 44, at 1548.

[97] Arthur Andersen LLP v. United States, 544 U.S. 696, 701–02 (2005).

[98] *Id.* at 708.

[99] *See id.* at 698 n.1.

Legal analysis can potentially achieve greater clarity by identifying overlooked sources of ambiguity. Anderson analyzes the *de re* and *de dicto* distinction through the lens of psycholinguistics and notes that a reflexive *de re* interpretation of an opaque sentence is consistent with cognitive processes favoring interpretations based on the world as it exists.[100] In the context of a law based on the mental state of the defendant, however, the world as it exists may be different than the world as imagined.[101] The presence of an opaque sentence therefore leads to what specialists in semantics call structural semantic ambiguity, and lawyers regularly only look for lexical and syntactic ambiguity.[102]

III. LAW AND INFLUENCE IN THE GREAT GAME

The previous Section discussed how language comes to mean something in laws. This Section zooms out on a different set of base assumptions about the origin of law, legitimacy, and power. Data breach laws are a useful vehicle for analyzing the legislative processes of states. As noted above, there is no unified federal response to data breaches as of this writing, and state data breach laws have emerged more or less organically, shaped strongly by industry input.

While Congress has been taking incremental steps to address cybersecurity in some contexts, states have served as a workshop for shaping data breach policy. Federal authority in this area is limited. There are breach disclosure requirements for medical information under the Health Insurance Portability and Accountability Act (HIPAA)[103] and for financial information in the Gramm-Leach-Bliley Act,[104] but there is no general data breach law. In *FTC v. Wyndham*, the Third Circuit recognized the power of the Federal Trade Commission to address data breaches based on the FTC's authority over matters of unfair business practices.[105] The FTC, though, is often limited in its range of enforcement options.

This Article is particularly concerned with outside sources of legislative text, including model and uniform legislation. Use of unorthodox lawmaking practices, like the use of outside drafters, has grown.[106] Such growth raises concerns about transparency, accountability, and democratic legitimacy.[107] As with most aspects of the law though, nuances abound. Unorthodox lawmaking practices may be more difficult to track, but there are many efficiency benefits to allowing flexibility. In the

---

[100] Anderson, *supra* note 44, at 1576.

[101] *Id.* at 1571.

[102] *Id.* at 1580.

[103] 15 U.S.C. § 6801(b) (2012).

[104] 45 C.F.R. §§ 164.400–.414 (2018).

[105] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015).

[106] Gluck et al., *supra* note 27, at 1823.

[107] *Id.* at 1812.

long run, this leads to an ongoing legal balancing act between accountability and effectiveness.

Early advocates for uniform laws emphasized that such laws helped avoid contradictory statutes.[108] According to one study, 34% of congressional staffers interviewed reported that the first drafts of legislation are typically written by policy experts and outside groups.[109] Federal agencies are another type of third party that might participate in legislation. Agencies are frequently consulted for technical drafting assistance on proposed legislation, and if the agency gives substantive contributions, there are transparency requirements that must be followed.[110] It is a settled norm that agencies will respond to virtually all requests for technical drafting assistance regardless of the policies implicated.[111]

Some model legislation is prepared by nonpartisan organizations like the Uniform Law Commission (ULC). Snyder likens the ULC to a "little legislature" given the organization's influence in policy adoption.[112] Past research has noted that uniform laws can increase efficiency in some legislative areas.[113] Professors Ribstein and Kobayashi found that the ULC's uniform legislation was especially attractive to states with part-time legislatures.[114] Special interest groups now lobby "little legislatures" in a way similar to their interactions with the official legislatures, raising concerns of capture.[115]

Federalism allows states to be legislative workshops. Competitive lawmaking enables what some call "molecular federalism."[116] However, Snyder warns that if competition fails, then molecular federalism instead signals the legislatures' abdication of their responsibilities.[117] A "market failure" in molecular federalism indicates either a need for more competitors in the market of legislative ideas, or a need for limitations on sources of external influence on legislatures.[118]

This Article also considers the contributions of the American Legislative Exchange Council (ALEC) to data breach laws. ALEC is a private organization that

---

[108] Frederic Jesup Stimson, *Uniform State Legislation*, 5 ANNALS AM. ACAD. POL. & SOC. SCI. 829, 830 (1895).

[109] Lisa Schultz Bressman & Abbe R. Gluck, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part II*, 66 STAN. L. REV. 725, 758 (2014).

[110] Walker, *supra* note 51, at 1389.

[111] *Id.* at 1390.

[112] Snyder, *supra* note 26, at 376.

[113] Larry E. Ribstein & Bruce H. Kobayashi, *An Economic Analysis of Uniform State Laws*, 25 J. LEGAL STUD. 131, 149–50 (1996).

[114] *Id.* at 187.

[115] *See* Snyder, *supra* note 26, at 435.

[116] *Id.* at 439.

[117] *Id.* at 449.

[118] *Id.*

provides model legislation to state legislatures in order to advance its members' pro-business interests.[119] ALEC is part of the trend to move to more networked governance models.[120]

Organizations that draft legislation outside of the government complicate matters of statutory interpretation, and this Section focuses on that external influence. Even assuming that something called "legislative intent" exists, is that intent affected by the origination of the language? This analysis goes to considerations of power, influence, and the legitimacy of the rule of law.

A. How an Idea Becomes a Bill Becomes a Law

This subsection proceeds as a sort of dialectic case study of privacy law. Data breach laws in particular lend themselves to analyses of the origins of law and legitimacy. This Article draws from the new legal realism movement in its focus on empiricism and broad contextual analysis of law.[121] As part of this focus, this subsection examines how new legal problems sometimes manifest as a feeling of discomfort with technology's new capabilities.

The invention of photography in the early 1800s allowed the fleeting to be made permanent. As photography technology improved and large-scale reproduction became possible, so too did nonconsensual use of images, like a business using another person's photo to advertise its product.[122] This led to common law developments like the misappropriation tort as well as statutory developments.[123]

In between the technology enabling a new use and the new use being addressed in a new law, there may be a distinct sense of discomfort,[124] which this Article calls the "squick factor." In popular terminology, "squick" describes a feeling somewhere between discomfort and disgust.[125] It is the point of the analysis at which someone says: "That behavior is legal, but it makes me uncomfortable."[126] It is a gut response to stimuli that does not necessarily imply moral judgment. Before image duplication was improved technologically, there was not much need for concern about rights in

---

[119] Rebecca Cooper et al., *Hidden Corporate Profits in the U.S. Prison System: The Unorthodox Policy-Making of the American Legislative Exchange Council*, 19 CONTEMP. J. REV. 380, 381 (2016).

[120] Anderson & Donchik, *supra* note 49, at 330.

[121] *See generally* Victoria Nourse & Gregory Shaffer, *Empiricism, Experimentalism, and Conditional Theory*, 67 SMU L. REV. 141 (2014).

[122] *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 385 (1960).

[123] *Id.*

[124] *See* Duhigg, *supra* note 23.

[125] *See Squick*, LEXICO, https://www.lexico.com/en/definition/squick (last visited Oct. 25, 2019).

[126] *See also supra* note 24 and accompanying text.

one's image. But then more uses became possible, and now there is a squick moment when a person sees his or her own face being used to enrich someone else.

Human behavior in the creation of laws can be visualized as proceeding in stages. Social and technological progress advances until a party voices discomfort and asks for redress. The squick thus marks the end of the first stage. The second stage is discourse. The offended party airs its grievances, and debates ensue about how society should address the situation.

This Article asserts that the discomfort associated with new photographic technologies parallels the discomfort associated with the loss of control over data. A lot of these changes began taking shape around the end of the 21st century. The internet was the new big thing. Businesses in all sectors started taking advantage of the new capabilities of a paperless, networked office. The destructive possibilities of poor security practices started to become more apparent, leading to the "squick" as sensitive information was exposed. States began adopting legislation to address what a business should do in the event of a security breach. The legislative adoption process took well over a decade, with the last state data breach laws adopted in 2018.

Thus, the behavioral context of lawmaking has three stages so far:

1. The Squick
2. The Discussion
3. The Adoption[127]

An adopted statute, though, is only mostly law. It exists in Schrodinger's box, where "use" refers simultaneously to using a gun only as a weapon and using a gun for bartering. Fundamentally, law is discourse, and under this Article's informal model, the law is not yet complete until it is applied.

The fourth major lawmaking behavior is thus the application of the law, which is generally associated with judges. With a statute, the goal in the application stage is to determine how the legislature's general directions should apply to an individual case. Lawmaking behavior can be plotted as a curve. Specific concerns are raised at the beginning, and the legislature works to craft rules that can address those concerns while taking broader contexts into account. By the time of judicial application, the specificity is again narrowed to the events of a particular violation. At that point, the focus is often on the violator instead of the offended party.

The lawmaking process can typically be deconstructed and traced back to some fundamental value, either cultural or universal. Internet policy discussions frequently discover a new squick enabled by technological developments. Data breaches are an obvious example. Identity theft has been possible for a long time, but before the growth of the internet and the creation of massive computerized databases of personal information, it was much less efficient. When millions of people

[127] Adoption either through common law or statute.

started trusting organizations with sensitive personal information, a trusted organization became a target and a single point of failure. Information privacy concerns focus on the connection between a person's identity and a person's data. The degree to which we identify with our data potentially indicates that legal responses to data breaches are driven by the value of personal autonomy.

Blackstone, in writing about sources of meaning in the law, recalls a case from antiquity involving vessel property rights.[128] At issue was a law that stripped property rights from ship owners who abandoned their ship in a storm. The ship then became the property of whoever stayed aboard. In the example case, there was a ship caught in a mighty tempest, and everyone who could escape the ship did so, leaving behind one sick passenger who was physically unable to leave. The plot twist is that the ship survived the storm and managed to drift safely into port, so the sick passenger claimed ownership of the ship. Blackstone notes that this is obviously not the reason for the law, because the sick passenger did nothing to protect the ship and was not incentivized to stay on the ship because of the law.[129] An alternative view is that forfeiture is still the just outcome because otherwise, ship operators would not be incentivized to look after sick passengers. This example shows that even laws that we think mean one thing can be valuable in unexpected ways and the main trick is our choice of perspective.

B. "The Room Where It Happens"[130]

Schoolhouse Rock was pretty optimistic in its explanation of how a bill becomes a law.[131] In the real world, legislating is often compared to a sausage factory. Even when the end result is quite palatable, witnessing the deal-making process might ruin one's appetite.

One of the basic concepts of negotiating is the existence of an anchor value. The first offer frequently serves to anchor future negotiations around that value. Viewed as a product of negotiations, the origin of legislative text becomes especially relevant. The first draft effectively anchors the negotiations, and future analysis of legislative history will probably start from there.

But where does the first draft come from? A lot of drafting is internal, and bills are often prepared by nonpartisan drafters in the state's legislative services office.[132]

---

[128] BLACKSTONE, *supra* note 45, at *61.

[129] *Id.*

[130] LIN-MANUEL MIRANDA, THE ROOM WHERE IT HAPPENS, *in* HAMILTON: AN AMERICAN MUSICAL (2015) ("No one really knows how the / Parties get to yes / The pieces that are sacrificed in / Ev'ry game of chess / We just assume that it happens / But no one else is in / The room where it happens.").

[131] Disney Educational Productions, *Schoolhouse Rock: America – I'm Just a Bill Music Video*, YOUTUBE (Dec. 8, 2011) https://www.youtube.com/watch?v=FFroMQlKiag.

[132] Hart, *supra* note 47, at 447.

Bill drafters sometimes borrow language from the statutes of other states and may also use model and uniform legislation.[133]

1. Outside Drafters

The previous subsection provided an informal deconstruction of how different concerns are raised throughout the lawmaking process. It showed that interactions between legislators and constituent groups are central to even begin the process. The legislator's job is to address these concerns, and, for reelection purposes, the legislator will likely choose the solution that causes the least harm—for a certain calculation of harm.

Studies about legislation show that legislators stay busy. The Sunlight Foundation found that in 2013, 5,584 bills were introduced in Congress, and only 56 were enacted.[134] Analysis by Quorum indicated that state legislatures introduce significantly more bills than does the Federal Congress, and enact these bills at much higher rates.[135] Quorum reports that in the first half of 2016, state legislatures enacted 24% of bills introduced.[136] This suggests that the workload of state legislators may be comparable in some respects to the workload of federal legislators, but with fewer cameras in the chamber.

This Article is especially concerned with state legislative actions and so seeks to appreciate the structure at work. The National Conference of State Legislatures has categorized state legislatures as full-time or part-time based on three major factors: lawmaker compensation, lawmaker time commitment, and legislative staffing.[137] As discussed above, though, state legislative productivity is frequently on par with (and by some measures exceeds) federal legislative productivity. To maintain this productivity, a part-time state legislature with fewer resources might be attracted to the idea of outsourcing legislative drafting. It is perhaps with this possibility in mind that several legislative drafting manuals include instructions for outside drafters.[138]

Some state legislation is initially drafted by private law-drafting groups. Some of this drafting is by long-established sources of model laws, like the American Legal Institute (ALI) and the ULC.[139] Relevant to this study, ALI currently has a project

---

[133] *Id.* at 447–48.

[134] Lee Drutman & Alexander Furnas, *Why Congress Might Be More Productive — and Less Partisan — Than You Think*, SUNLIGHT FOUND. (Jan. 16, 2014), https://sunlightfoundation.com/2014/01/16/congress-in-2013/.

[135] Kevin King, *State Legislatures vs. Congress: Which Is More Productive?*, QUORUM, https://www.quorum.us/data-driven-insights/state-legislatures-versus-congress-which-is-more-productive/176/ (last visited Oct. 25, 2019).

[136] *Id.*

[137] *Full — and Part — Time Legislatures*, NAT'L CONF. ST. LEGIS. (June 14, 2017), http://www.ncsl.org/research/about-state-legislatures/full-and-part-time-legislatures.aspx.

[138] Hart, *supra* note 47, at 452.

[139] Orbach, *supra* note 78, at 2.

dedicated to data privacy principles,[140] and ULC appears to be in the early stages of a project to create a uniform data breach law.[141]

In some situations, uniformity is especially desirable. Some argue that ULC's uniform law expertise should be concentrated on procedural, commercial, and probate statutes.[142] As an inherently multijurisdictional issue tied to commercial law, data breach statutes are arguably strong candidates for uniformity.

When the private sector provides statutory language, though, possible sources of bias should be addressed. In addition to long-established private drafting groups, there are also newer players that represent a kind of "policy entrepreneurship" approach to civic engagement.[143] The American Legislative Exchange Council (ALEC) is perhaps the most dominant of these groups, with state legislatures annually introducing about 1,000 bills derived from ALEC's model laws.[144] The enactment rate of ALEC-sourced bills is reportedly between 14 and 20 percent.[145]

ALEC is an organization that was formed in 1973 to advance policies favoring businesses and certain free market principles.[146] One of ALEC's co-founders is Paul Weyrich, who co-founded other notable conservative institutions like The Heritage Foundation and The Moral Majority.[147] ALEC membership includes legislators, corporations, private foundations, and trade associations.[148] Koch Industries and the National Rifle Association are major contributors to ALEC.[149] ALEC, along with the National Rifle Association's Institute for Legislative Action, is associated with many state stand-your-ground laws.[150]

---

[140] *Principles of the Law: Data Privacy*, AM. L. INST. ADVISER, http://www.thealiadviser.org/data-privacy (last visited Oct. 25, 2019).

[141] ANNUAL MEETING OF THE COMMITTEE ON SCOPE AND PROGRAM, UNIFORM L. COMM'N (July 2018), https://my.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=4be48d27-ee5b-6a1e-cfff-91af6ae4d0af&forceDialog=0.

[142] Ribstein & Kobayashi, *supra* note 113, at 149–50.

[143] Anderson & Donchik, *supra* note 49, at 334–35 (noting that with policy entrepreneurs, it can be hard to tell when policy advocacy ends and profit-seeking begins).

[144] Hart, *supra* note 47, at 448.

[145] Cooper et al., *supra* note 119, at 385 (citing a 14% enactment rate); Hart, *supra* note 47, at 448 (citing an approximately 20% enactment rate); Tang, *supra* note 35, at 1482 (citing a 17% enactment rate).

[146] Cooper et al., *supra* note 119, at 381; Dane E. Johnson, *Cages, Clinics, and Consequences: The Chilling Problems of Controlling Special-Interest Extremism*, 86 OR. L. REV. 249, 255 (2007).

[147] Cooper et al., *supra* note 119, at 381.

[148] *Id.* at 382 (also noting that the membership fee for legislators is much smaller than the membership fee for private organizations).

[149] Anderson & Donchik, *supra* note 49, at 338; Lisa Graves, *ALEC Exposed: The Koch Connection*, NATION (July 12, 2011), https://www.thenation.com/article/alec-exposed-koch-connection/.

[150] Orbach, *supra* note 78, at 3.

ALEC is registered as a 501(c)(3) nonprofit organization, though some groups have challenged ALEC's tax exempt status in recent years.[151] ALEC is funded in part by private businesses and behaves like a lobbying organization in some ways, but also has traits of the government sector due to legislator participation.[152]

In law school, students are generally taught to seek objectivity. In popular culture, judges are praised as neutral arbiters of the law. However, pressure from special interest groups frequently compromises objectivity in legislative drafting. The ULC has been criticized for its susceptibility to interest group pressure and a pro-business bias.[153] But the ULC arguably at least strives for objectivity. ALEC, on the other hand, embraces a pro-business bias in the interest of advocacy. Critics warn that the use of model bills allows ALEC to obscure its members' profit motives.[154] ALEC has responded to some criticism by pointing out that many state legislators are only part-time lawmakers, and so ALEC is providing a valuable service.[155]

This does not obscure the fact that ALEC is also providing a valuable service for lobbyists, for whom focusing on state legislation makes a lot of strategic sense.[156] Indeed, ALEC is all about strategy. Some have accused ALEC of pushing decoy bills that are designed to distract the media from covering other bills that it wants to pass.[157] Legal reasoning is founded on a useful fiction that ideas are related to each other in some impartial way, so clear partiality in the creation of laws deserves scrutiny.

2. Interest Groups

It is not controversial to acknowledge the role of interest groups in government. One 2012 study examined 14 issue areas and found that interest groups frequently influence major policy enactments.[158] The percentage of significant enactments with interest group influence ranged from 30.8% in criminal justice policy to 69.1% in environmental policy.[159]

---

[151] *See, e.g.*, David Vance, *New Allegations of Tax Code Violations by Exxon and ALEC Filed with IRS*, COMMON CAUSE (Oct. 6, 2016), https://www.commoncause.org/media/new-allegations-of-tax-code-violations-by-exxon-and-alec/.

[152] Anderson & Donchik, *supra* note 49, at 348.

[153] Ribstein & Kobayashi, *supra* note 113, at 145.

[154] Cooper et al., *supra* note 119, at 384.

[155] Lois Beckett, *A Discreet Nonprofit Brings Together Politicians and Corporations to Write "Model Bills,"* PROPUBLICA (July 15, 2011), https://www.propublica.org/article/a-discreet-nonprofit-brings-together-politicians-and-corporations-to-write-.

[156] Anderson & Donchik, *supra* note 49, at 340.

[157] *Id.* at 341.

[158] Matt Grossman, *Interest Group Influence on US Policy Change: An Assessment Based on Policy History*, 1 INT. GROUPS & ADVOC. 171, 171 (2012).

[159] *Id.* at 181.

In *Citizens United v. FEC*, the Supreme Court empowered interest groups to get more monetarily involved in the political process. This was based in part on the theory that prohibiting restrictions on individual political expenditures made legislatures more accountable to the people.[160] On the other hand, such unlimited expenditures may also run the risk of making legislatures more accountable to special interests *at the expense of* the people.[161] In the case of what Orbach calls "interested private lawmaking,"[162] draft bills prepared by outside organizations are far from transparent.[163] One of the things that makes legislative sausage more palatable is knowing that the legislators promoting the policy are ultimately accountable to their constituents. Bills drafted by pressure groups, then, lack the same democratic legitimacy.[164]

ALEC provides many networking benefits to mutually aligned interest groups to help them achieve their policy goals. In 2011, a whistleblower leaked hundreds of internal ALEC documents to the Center for Media and Democracy.[165] This leak was the source used by several empirical examinations of ALEC's proposed bills.[166] ALEC provides policy advocacy services that tend to lean right, which would be less problematic in a competitive market of ideas. However, current progressive advocacy networks are not providing meaningful competition, which some blame on these networks' lack of an ideological alliance.[167]

At the federal level, ALEC supported the passage of the Animal Enterprise Terrorism Act that extended the "terrorist" designation to protesters who interfere with animal enterprises.[168] At the state level, ALEC makes extensive efforts relating to education and prisons. Some have concluded that ALEC acts "with the goal of privatizing and marketizing public education."[169] ALEC also applies discursive strategies, often using words like "freedom" and "choice" in its education bills.[170] Prison-related bills accounted for almost 20% of the ALEC bills leaked in 2011.[171] These bills addressed private prisons, private goods and services in prisons, the use of prison

---

[160] Orbach, *supra* note 78, at 5.

[161] *Id.* at 15–16 ("In the marketplace of ideas, unleashed interest groups may have effective means to influence public lawmakers to be accountable to *their people* at the expense of *the people*.").

[162] Orbach, *supra* note 78, at 15.

[163] Cooper et al., *supra* note 119, at 393.

[164] Orbach, *supra* note 78, at 10.

[165] Cooper et al., *supra* note 119, at 384.

[166] Anderson & Donchik, *supra* note 49, at 324; Cooper et al., *supra* note 119, at 386.

[167] Anderson & Donchik, *supra* note 49, at 350.

[168] Kimberly E. McCoy, *Subverting Justice: An Indictment of the Animal Enterprise Terrorism Act*, 14 ANIMAL L. 53, 58 (2007).

[169] Anderson & Donchik, *supra* note 49, at 322.

[170] *Id.* at 345.

[171] Cooper et al., *supra* note 119, at 386.

labor, and increasing the prison population. They are often framed as public safety measures, but for many of those involved, they are merely business transactions.[172]

C. *Influence and Legislation*

In a perfect world, voters would be informed without being manipulated and policy decisions would be made based on merit. Unfortunately, most voters remain uninformed and are more easily swayed by well-funded political messaging.[173] Policy battles are often not won based on merit, but instead on who frames the issue best.[174] In our imperfect world, additional controls are needed to prevent abuses of power. The Supreme Court has long recognized that politically powerless classes must be protected from the majoritarian political process.[175]

Political process theory is a long-recognized doctrine related to the Equal Protection clause of the Fourteenth Amendment and indicates that judges should apply heightened judicial scrutiny to government actions affecting the political process.[176] One category of political process theory cases concerns placing restrictions on the adoption of antidiscrimination ordinances.[177] In *Romer v. Evans*, the Supreme Court reviewed a state constitutional amendment passed by a majority of Colorado voters. The amendment prohibited any government action made to protect individuals based on their "homosexual, lesbian or bisexual orientation, conduct, practices or relationships."[178]

At the core of political process theory is the recognition that while a law may frequently disfavor *somebody*, the real question is whether that person was disfavored

---

[172] *Id.* at 388 (quoting Jerry Watson, senior legal counsel at ABC, at an ALEC conference: "I'm not so crazy as not to know that you've already figured out that if I can talk you into doing this bill, my clients are going to make some money on the bond premiums . . . but if we can help you save crime victims in your legislative district and generate positive revenue for your state, and help solve your prison overcrowding problem, you don't mind me making a dollar."); *see also* Laura Sullivan, *Prison Economics Help Drive Ariz. Immigration Law*, NAT'L PUB. RADIO (Oct. 28, 2010), https://www.npr.org/2010/10/28/130833741/prison-economics-help-drive-ariz-immigration-lawViguerie.

[173] Gluck et al., *supra* note 27, at 1842.

[174] Anderson & Donchik, *supra* note 49, at 352.

[175] *See* San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1, 28 (1973).

[176] *E.g.*, Hunter v. Erickson, 393 U.S. 385, 391 (1969) (evaluating a city charter provision requiring that anti-discrimination housing ordinances be approved by a majority of voters); *see also* Kristen Barnes, *Breaking the Cycle: Countering Voter Initiatives and the Underrepresentation of Racial Minorities in the Political Process*, 12 DUKE J. CONST. L. & PUB. POL'Y 123, 129 (2017); Tang, *supra* note 35, at 1431.

[177] *E.g.*, Romer v. Evans, 517 U.S. 620, 620 (1996); *Hunter*, 393 U.S. at 390.

[178] COLO. CONST. art. 2, § 30b (West, Westlaw through Nov. 6, 2018 amendments); *Romer*, 517 U.S. at 624.

fairly or unfairly.[179] Tang notes a trend in recent Supreme Court cases that he terms "reverse political process theory," where politically powerful groups may have stronger constitutional protections than politically powerless groups.[180]

But as long as the complaints are not too loud, influential interest groups play a healthy role in the governing process. Arthur Bentley examined a variety of topics relating to human behavior, law, and government, and observed that law was driven by pressure.[181] Similarly, economist Gary Becker argued that political equilibrium is determined by how different groups produce pressure.[182] In a pluralist society, each individual can belong to several groups, and different groups may have different and sometimes conflicting goals. Each group is assumed to act for the well-being of its members in pursuing political influence.[183] In a pluralist democracy, therefore, supporters of legislation often need to build a coalition with other groups to achieve a majority. Becker's characterization, however, is built on the assumption that group membership is authentic and not strategic.

In a pluralist democracy, each person is a member of many different groups, and these groups are affected by government policies. In a well-functioning pluralist democracy, alliances across groups are necessary to achieve a majority of support for a new policy.[184] Nicolas Stephanopoulos defines a group as politically powerless "if its aggregate policy preferences are less likely to be enacted than those of similarly sized and classified groups."[185] Stephanopoulos asserts that "in a properly functioning political system, groups of about the same size and type should have about the same odds of getting their preferred policies enacted."[186] If a group sees its preferred policies enacted at a rate significantly lower than other groups of comparable size, such results indicate that something is not working properly.[187] The corollary to this assertion is that it may also indicate dysfunction if a group rarely sees its preferred policies rejected.

Becker analyzes political pressure as a zero-sum game. His economic analysis indicates that if subsidies and taxes are both greater than zero, the people who are subsidized are the winners and the people who are taxed are the losers.[188] When

---

[179] Tang, *supra* note 35, at 1442–43.

[180] *Id.* at 1428.

[181] BENTLEY, *supra* note 34, at 296.

[182] Gary S. Becker, *A Theory of Competition Among Pressure Groups for Political Influence*, 98 Q.J. ECON. 371, 371 (1983). Political equilibrium refers to a state in which all groups have optimized the amount they spend on political pressure. *Id.* at 372.

[183] *Id.* at 372.

[184] Nicholas O. Stephanopoulos, *Political Powerlessness*, 90 N.Y.U. L. REV. 1527, 1547 (2015).

[185] *Id.* at 1531.

[186] *Id.* at 1545.

[187] *Id.*

[188] Becker, *supra* note 182, at 376.

taxes are broadly distributed, however, opposition will probably decrease because there is less of an impact on a per capita basis.[189] Becker posits that "a group that becomes more efficient at producing political pressure would be able to reduce its taxes or raise its subsidy."[190]

In a 1991 article, William Eskridge analyzed Supreme Court cases and subsequent overriding legislation enacted between 1967 and 1990. He found that organized worker groups like unions tended to be more successful than big business interests at convincing Congress to overturn the high court's statutory interpretation decisions.[191] Almost 30 years later, some might suggest that the pendulum has now swung the other way in terms of which party has more political sway.[192] This political ebb and flow is important for legal practitioners to observe, because law is never practiced in a vacuum, but instead as the result of prolonged ideological and sociological evolution. Data breach laws provide an opportunity to examine a snapshot of this phenomenon, as the "squick" of data insecurity pits pressure groups against each other in the state legislative process.

IV. DATA BREACH LAWS

State data breach laws generally proceed in predictable ways. The breach is the triggering event, and some items may be excluded from the definition of a breach.

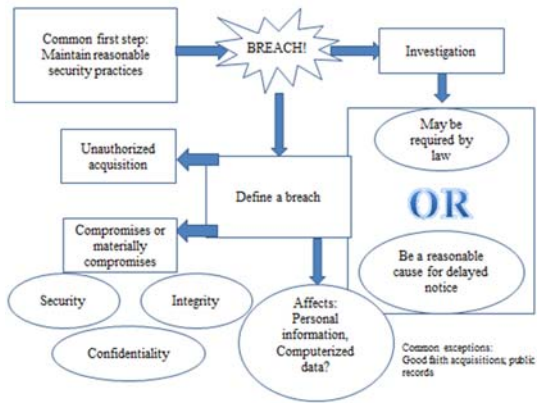

Figure 1. Diagramming data breach laws

Protected classes of information are enumerated, and some types of information are excluded. Notifications are required to be sent to affected individuals, except when they are not. The themes of data breach laws are fairly consistent across the country,

[189] *Id.* at 384.

[190] *Id.* at 380.

[191] William N. Eskridge, Jr., *Overriding Supreme Court Statutory Interpretation Decisions*, 101 YALE L.J. 331, 352 (1991).

[192] *See generally* Tang, *supra* note 35.

but the small differences and ambiguities accumulate. These small differences may contribute to the high cost of responding to data breaches in the United States.

A. Methodology

This Article's study proceeds with the underlying assumption that language can be quantified. Data breach laws were analyzed and coded based on content.[193] Analysis included 50 state laws, the data breach law of the District of Columbia, and a model data breach law proposed by a private organization. Progress was tracked in a spreadsheet. Linguistic analysis led to the creation of 121 columns, which can be placed into eight categories: 1) General information; 2) Enforcement; 3) Notification requirements; 4) Security requirements; 5) Personal information; 6) Breaches; 7) Interaction with other laws; and 8) Miscellaneous. The column headings are listed in the appendix according to these eight categories. These 121 headings will be generally referred to as traits of the laws. Most of these are what the author considers "hard-coded" traits—that is, the trait is phrased in such a way that responses are coded as either yes or no, sometimes with qualifications.

There are also some "soft-coded" traits when qualitative descriptions are more useful. Thresholds, for example, are more helpfully described with soft-coding, such as:

1. What is the time limit for a data breach notification?
2. How many people should be affected by a breach before the state Attorney General must be notified?
3. At what point is the cost of notification high enough that substitute notice becomes available?

In data breach laws, legislators often set threshold values that communicate a range of priorities. This is especially clear with enforcement. One state might require the Attorney General (AG) to be notified of any potential breach, and another might only require AG involvement after notice is determined to be required for over a threshold number of state residents.

Each data breach law was read at least twice. Much like how a law professor might read every essay response once before starting to rank and quantify answers, comparative statutory analysis increases in clarity as more examples become available. In the case of data breach laws, the current comparative approach evolved as the differences between seemingly minor drafting choices formed patterns in the aggregate.

By forging a new trail with comparative data breach law analysis, this Article supplements current research into data security policy. Data breaches are generally

---

[193] *See generally* JOHNNY SALDAÑA, THE CODING MANUAL FOR QUALITATIVE RESEARCHERS (Jai Seaman, 2d ed. 2013).

defined as an unauthorized acquisition of unencrypted electronic data that compromises the security, confidentiality, or integrity of data. There are, however, many slight alterations to even this general definition. Some states refer to the unauthorized access, release, or use of data. Alabama, New York, and Vermont provide some guidelines for how to tell if unauthorized acquisition has occurred.[194] Some states do not limit breaches to just electronic data, so a stolen box of paper documents might also trigger notification requirements. Some states do not mention security, confidentiality, or integrity. Some only mention security and confidentiality. These differences are the result of affirmative choices by state legislators.

B. Step 0: Why?

Analysis of statutory trends must consider the purpose of the law. Punitive laws can either have a victim-centered purpose or a perpetrator-centered purpose. In the case of data breach laws, legislatures overwhelmingly focus on the commerce or consumer protection implications. Data breach notification laws are thus generally imbued with a victim-centered purpose. Previous work on this topic has examined the nature of the injury caused by a data breach.[195] Recent scholarship has argued that data insecurity causes anxiety on the part of victims whose sensitive information has been compromised.[196] Laws governing data breaches should thus emphasize the implications for victims who for our purposes will generally be referred to as "data subjects."

Data breach laws are often couched in terms of preventing identity theft. But what is the social value that we protect with identity theft laws? Is the emphasis on protecting the individual or punishing the wrongdoer? Identity theft laws are often inconsistent on this point. The general wisdom is that identity theft laws are victim-centered, and many identity theft laws address specific remedies available to identity theft victims, like identity theft passports. On the other hand, a review of state identity theft laws finds that eighteen states include pretending to be a dead person as identity theft, in which case the motivation to protect the victim is weaker. More significantly, at least five states recognize the crime of identity theft when the "stolen" identity is fictitious,[197] and eleven states recognize the crime of identity theft

---

[194] ALA. CODE § 8-38-4(b) (2019); N.Y. GEN. BUS. LAW § 899-aa(c) (McKinney 2019); VT. STAT. ANN. tit. 9, § 2430(8)(C) (2019).

[195] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 737 (2018).

[196] *Id.* at 763–64.

[197] ARIZ. REV. STAT. ANN. § 13-2008 (2019); IND. CODE § 35-43-5-3.8 (2019); NEV. REV. STAT. § 205.4653 (2017); OR. REV. STAT. § 165.813 (2017); VA. CODE ANN. § 18.2-186.3 (2019).

when the stolen identity is used to obtain employment.[198] In those two situations, a victim-centered analysis falls apart because the injury is ambiguous at best. Including the use of a stolen identity to obtain employment is most likely a reference to undocumented laborers, and pretending to be a fake person only potentially harms the person being deceived.

Statutory organization is an element of statutory interpretation that is often ignored, but it can be informative in discerning the underlying purpose. Data breach laws are most often situated either in a consumer protection or trade regulation code section. This indicates that data breaches are seen as an economic issue in these states. On the other hand, four states placed their data breach notification laws within a statutory section on crime,[199] and four states placed data breach provisions in code sections about network security or privacy.[200] These placements suggest a focus on the data subject as something other than an economic actor. Of course, placement does not always signal content. Arizona examines data breaches under the same statutory chapter as other network security issues and has an entire title of its state code dedicated to information technology.[201] Yet in spite of this contextual focus on information technology, Arizona's data breach law does not require covered entities to adopt reasonable security measures.

C. Step 1: Prevention

A federal or model data breach law needs to address preventative measures in addition to notification requirements. Encryption is a bare minimum practice that almost all states include in their data breach laws. Wyoming is the singular exception, as the language of the Wyoming statute only refers to redaction of personal information, not encryption.[202]

Most often, encryption is addressed in the context of when a notification is *not* required, but it is discussed in this Section because encryption is a basic preventative measure. The data breach law in the District of Columbia does not require notification if the data was "rendered secure,"[203] which can fairly be read as including

---

[198] ALA. CODE § 13A-8-192; ARIZ. REV. STAT. ANN. § 13-2008 (2019); GA. CODE ANN. § 16-9-121.1 (2019); MICH. COMP. LAWS § 445.65 (2019); MISS. CODE ANN. § 97-19-85 (2018); NEB. REV. STAT. § 28-639 (2019); N.D. CENT. CODE § 12.1-23-11(3) (2019); S.C. CODE ANN. § 16-13-510 (2018); UTAH CODE ANN. § 76-6-1102 (West 2019); W. VA. CODE ANN. § 61-3-54 (2017); WIS. STAT. § 943.201 (2017).

[199] IOWA CODE §§ 715C.1–715C.2 (2019); 11 R.I. GEN. LAWS §§ 11-49.3-1 to -6 (2019); S.D. CODIFIED LAWS §§ 22-40-19 to -26 (2018); VA. CODE ANN. § 18.2-186.6.

[200] ALASKA STAT. §§ 45.48.010–.090 (2019); ARIZ. REV. STAT. §§ 18-551 to -552; NEV. REV. STAT. §§ 603A.010–.290; N.H. REV. STAT. §§ 359-C:19 to -C:21 (2019).

[201] ARIZ. REV. STAT. §§ 18-552.

[202] WYO. STAT. ANN. § 40-12-501(a)(i) (2019).

[203] D.C. CODE § 28-3851(1) (2019).

encryption. Twenty-seven states require notification when encrypted information is affected if the means of decrypting the data was also included in the breach.[204]

State data breach laws that address prevention may also do so by requiring reasonable security practices, as 16 states do,[205] or by addressing the disposal of records, as is the case in 23 states.[206] Records disposal can be and often is addressed elsewhere in a state's code, but for this study, only records disposal provisions that were in the textual proximity of data breach laws were counted. Nevada is one of the states that requires some reasonable security practices, but Nevada also goes further by exempting entities from data breach liability if they comply with the security requirements and if the breach incident was not caused by gross negligence.[207]

Of the 16 states that require the adoption of reasonable security practices, eight states also require covered entities to ensure that the third parties they send data to have reasonable security measures.[208] Oregon does not address data transfers

[204] ALA. CODE § 8-38-2 (2019); ALASKA STAT. § 45.48.090; CAL. CIV. CODE § 1798.82 (West 2019); COLO. REV. STAT. § 6-1-716 (2019); DEL. CODE ANN. tit. 6, § 12B-101 (2019); HAW. REV. STAT. § 487N-1 (2019); 815 ILL. COMP. STAT. 530/5 (2019); IND. CODE § 24-4.9-2-2 (2019); IOWA CODE § 715C.1; MASS. GEN. LAWS ch. 93I, § 1 (2019); MICH. COMP. LAWS § 445.72 (2019); MINN. STAT. § 325E.61 (2019); NEB. REV. STAT. § 87-802 (2019); N.H. REV. STAT. ANN. § 359-C:19; N.M. STAT. ANN. § 57-12C-2 (2019); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); N.C. GEN. STAT. § 75-61 (2018); OK. STAT. tit. 24, § 163 (2019); OR. REV. STAT. § 646A.602 (2017); 73 PA. STAT. § 2303 (2019); 11 R.I. GEN. LAWS § 11-49.3-3; S.D. CODIFIED LAWS § 22-40-19; TENN. CODE § 47-18-2107 (2019); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2019); VA. CODE ANN. § 18.2-186.6; WASH. REV. CODE § 19.255.010 (2019); W. VA. CODE ANN. § 46A-2A-102 (2017).

[205] ALA. CODE § 8-38-3; ARK. CODE ANN. § 4-110-104; CAL. CIV. CODE § 1798.81.5; COLO. REV. STAT. § 6–1–713.5; FLA. STAT. § 501.171(2); 815 ILL. COMP. STAT. 530/45; IND. CODE § 24-4.9-3-3.5; LA. STAT. ANN. § 3074; MD. CODE ANN., COM. LAW § 14-3503 (2018); 201 MASS. CODE REGS. § 17.03; NEB. REV. STAT. § 87-808; NEV. REV. STAT. § 603A.210; N.M. STAT. ANN. § 57-12C-4; OR. REV. STAT. § 646A.622; 11 R.I. GEN. LAWS § 11-49.3-2; TEX. BUS. & COM. CODE ANN. § 521.052; UTAH CODE ANN. § 13-44-201 (West 2019).

[206] ALA. CODE 8-38-10; ARK. CODE ANN. § 4-110-104; CAL. CIV. CODE § 1798.81; COLO. REV. STAT. § 6-1-713; FLA. STAT. § 501.171; HAW. REV. STAT. § 487R-2; 815 ILL. COMP. STAT. 530/40; IND. CODE § 24-4.9-3-3.5; KY. REV. STAT. ANN. § 365.725 (West 2019); LA. STAT. ANN. § 3074; MD. CODE ANN., COM. LAW § 14-3502; MASS. GEN. LAWS ch. 93I, § 2; MICH. COMP. LAWS § 445.72a; MONT. CODE ANN. § 30-14-1703 (2019); NEB. REV. STAT. § 87-808 (referring to the requirement of having a records disposal process in place, but without providing specific requirements); NEV. REV. STAT. § 603A.200; N.J. STAT. ANN. § 56:8-162; N.M. STAT. ANN. § 57-12C-3; N.C. GEN. STAT. § 75-64; OR. REV. STAT. § 646A.622; 11 R.I. GEN. LAWS § 11-49.3-2; TEX. BUS. & COM. CODE ANN. § 521.052 (records disposal at private businesses); TEX. GOV'T CODE ANN. § 2054.130 (records disposal at government agencies); UTAH CODE ANN. § 13-44-201; VT. STAT. ANN. tit. 9, § 2445 (2019).

[207] NEV. REV. STAT. § 603A.215(3)(b).

[208] COLO. REV. STAT. § 6-1-713.5; 815 ILL. COMP. STAT. 530/45; MD. CODE ANN., COM. LAW § 14-3503; 201 MASS. CODE REGS. § 17.03 (2018); NEB. REV. STAT. § 87-808; NEV. REV. STAT. § 603A.210; N.M. STAT. ANN. § 57-12C-5; 11 R.I. GEN. LAWS § 11-49.3-2.

broadly, but requires "service providers" that work with the covered entity to be subject to contract terms requiring safeguards and practices to protect personal information.[209]

Massachusetts[210] and Oregon[211] have the most detailed security requirements among state data breach laws. Of the two, Massachusetts is more detailed about technology, and Oregon is more detailed about administrative protocol. Massachusetts requires secure authentication protocols, secure access control measures, encryption, ongoing monitoring of systems that contain personal information, firewalls to protect systems that contain personal information, up-to-date antivirus software, and employee education on the security of personal information.[212] Oregon requires three categories of protection: administrative safeguards, technical safeguards, and physical safeguards. Administrative safeguards include employee training, regular review of user access privileges, and risk management practices. Technical safeguards include security updates, regular tests of the effectiveness of security, and requirements to monitor, detect, prevent, and respond to cyberattacks and system failures. Physical safeguards include relevant risk assessment, monitoring, and safeguards for the disposal of records.[213]

D. Step 2: The Breach

Data breach statutes are activated by security events. In analyzing statutory language, attention was paid to how the statutes defined a breach of security. A majority of statutes, 28 of 51, defined a breach as an incident that "compromises the security, confidentiality, or integrity" (SCI) of protected information.[214] Seven states require

---

[209] OR. REV. STAT. § 646A.622(1).

[210] 201 MASS. CODE REGS. § 17.00–.04.

[211] OR. REV. STAT. § 646A.622.

[212] 201 MASS. CODE REGS. § 17.03–.04.

[213] OR. REV. STAT. § 646A.622(2)(d)(A)–(C).

[214] ALASKA STAT. § 45.48.090 (2019); ARK. CODE ANN. § 4-110-103 (2019); CAL. CIV. CODE § 1798.82 (West 2019); COLO. REV. STAT. § 6-1-716 (2019); DEL. CODE ANN. tit. 6, § 12B-101 (2019); D.C. CODE § 28-3851 (2019); GA. CODE ANN. § 10-1-911 (2019); 815 ILL. COMP. STAT. 530/5 (2019); IND. CODE § 24-4.9-2-2 (2019); IOWA CODE § 715C.1 (2019); KAN. STAT. ANN. § 50-7a01 (2018); KY. REV. STAT. ANN. § 365.732 (West 2019); LA. STAT. ANN. § 3073; ME. REV. STAT. ANN. tit. 10, § 1347 (2019); MD. CODE ANN., COM. LAW § 14-3504 (2018); MASS. GEN. LAWS ch. 93H, § 1 (2019); MINN. STAT. § 325E.61 (2019); MO. REV. STAT. § 407.1500 (2019); NEB. REV. STAT. § 87-802 (2019); N.J. STAT. ANN. § 56:8-161; N.M. STAT. ANN. § 57-12C-2 (2019); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); 11 R.I. GEN. LAWS § 11-49.3-3 (2019); S.C. CODE ANN. § 39-1-90 (2018); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2019); UTAH CODE ANN. § 13-44-102 (West 2019); VT. STAT. ANN. tit. 9, § 2430 (2019); WASH. REV. CODE § 19.255.010 (2019).

that the incident "materially" compromise the SCI of protected information.[215] Eight states omit data integrity as a factor.[216] In two of those eight, the incident must materially compromise the security or confidentiality of protected information.[217] Eight other states do not include SCI language in their definition of a breach of security.[218]

A wide majority, 50 of 51, tie breaches to the unauthorized acquisition of protected data. Sixteen states tie breaches to the unauthorized access to protected data.[219] Of those 16, New Jersey is the only one that does not also connect breaches to unauthorized acquisition.[220] Maine and North Carolina include the unauthorized release of information in their breach definitions, and unauthorized use is part of the breach definition in both Maine and Massachusetts.[221] Alabama, New York, and Vermont include some guidelines for determining whether protected information has been subjected to unauthorized acquisition.[222]

Data breach laws are almost always focused on the breach of personal information that could facilitate identity theft. The standard formula is the last name and first initial plus a social security number, driver's license number, or financial account information and the means to access that account, such as a password or

---

[215] IDAHO CODE §§ 28-51-104 (2019); MONT. CODE ANN. § 30-14-1704 (2019); NEV. REV. STAT. § 603A.020 (2017); OR. REV. STAT. § 646A.602; S.D. CODIFIED LAWS § 22-40-19 (2018); TENN. CODE § 47-18-2107 (2019); WYO. STAT. ANN. § 40-12-501 (2019).

[216] ARIZ. REV. STAT. ANN. § 18-545; MICH. COMP. LAWS § 445.63 (2019); N.H. REV. STAT. ANN. § 359-C:19 (2019); OHIO REV. CODE ANN. § 1349.19 (West 2019); OK. STAT. tit. 24, § 162 (2019); 73 PA. STAT. § 2302 (2019); VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-101 (2017).

[217] ARIZ. REV. STAT. ANN. § 18-54; 73 PA. STAT. § 2302.

[218] ALA. CODE § 8-38-2 (2019); CONN. GEN. STAT. § 36a-701b (2019); FLA. STAT. § 501.171(1) (2019); HAW. REV. STAT. § 487N-1 (2019); MISS. CODE ANN. § 75-24-29 (2018); N.C. GEN. STAT. § 75-61 (2018); N.D. CENT. CODE ANN. § 51-30-01 (2019); WIS. STAT. § 134.98 (2017).

[219] ARIZ. REV. STAT. ANN. § 18-551; CONN. GEN. STAT. § 36a-701b; HAW. REV. STAT. § 487N-1; KAN. STAT. ANN. § 50-7a01; LA. STAT. ANN. § 3073; MICH. COMP. LAWS § 445.63; MO. ANN. STAT. § 407.1500; N.J. STAT. ANN. § 56:8-161; N.C. GEN. STAT. § 75-61; OHIO REV. CODE ANN. § 1349.19; OK. STAT. tit. 24, § 162; 73 PA. STAT. § 2302; 11 R.I. GEN. LAWS § 11-49.3-3; S.C. CODE ANN. § 39-1-90; VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-101.

[220] N.J. STAT. ANN. § 56:8-161.

[221] MASS. GEN. LAWS ch. 93H, § 1 (2019); ME. REV. STAT. ANN. tit. 10, § 1347(1) (2019); N.C. GEN. STAT. § 75-61(14).

[222] ALA. CODE § 8-38-4(b); N.Y. GEN. BUS. LAW § 899-aa(c) (McKinney 2019); VT. STAT. ANN. tit. 9, § 2430(8)(C) (2019).

PIN. Biometric data is included in the definition of personal information in a minority of states, including Arizona, Colorado, and Illinois.[223] In Connecticut, biometric data is listed as a protected type of "confidential information" in Section 4e-70, which pertains to state contractors who receive confidential information, but *not* as a type of "personal information" under Section 36a-701b, which is the state's primary data breach law.[224] Delaware and Wisconsin include not just biometric indicators, but also an individual's DNA profile as an example of personal information.[225]

Data breach laws often focus on "personal information," though some use the term "personal identifying information." Michigan's law defines the two terms separately and uses "personal identifying information" in the provisions about the commission of identity theft crimes.[226] The more narrowly defined "personal information" appears in the data breach notification law and is defined by the standard formula presented above: name, social security number, driver's license number, and financial account information.[227] Michigan's definition of "personally identifiable information" includes additional elements, including mother's maiden name, passport number, and biometric data.[228] Thus in Michigan, biometric data is relevant for the crime of identity theft, but not for the data breach notification law.

Data breach laws also include exceptions. Two prominent exceptions that almost always appear are the good faith employee exception and the public records exception. The good faith employee exception typically appears in the statute's definition of a breach and says that it does not count as a breach if a good faith employee acquired the personal information and there was no subsequent misuse of the information. Forty-seven states and the District of Columbia include this exception.[229] Oregon uses a less permissive form of this exception, only excluding the inadvertent acquisition by employees, not good faith acquisition.[230]

The public records exception typically appears in the definition of personal information and says that information from public records does not count as personal information for the purpose of the data breach law. This exception is worded

---

[223] ARIZ. REV. STAT. ANN. § 18-551(7)(a)(i), (11)(i); COLO. REV. STAT. § 6-1-713(2) (2019); 815 ILL. COMP. STAT. 530/5(F) (2019).

[224] CONN. GEN. STAT. §§ 4e-70, 36a-701b (2019).

[225] DEL. CODE ANN. tit. 6, § 12B-101 (2019); WIS. STAT. § 134.98(1)(b) (2017).

[226] MICH. COMP. LAWS § 445.63(r) (2019).

[227] *Id.* § 445.72.

[228] *Id.* § 445.63(q).

[229] The three states that do not include an exception for good faith acquisition by an employee are Connecticut, Mississippi, and Oregon. Of these three, Oregon includes a similar exception for inadvertent acquisition but not an exception for good faith acquisition. OR. REV. STAT. § 646A.602 (2017).

[230] OR. REV. STAT. § 646A.602(1)(b).

to apply to government records. Public records generally include information "lawfully made available to the general public from federal, state, or local government records."[231] Twenty-two states also consider sources other than government records to be part of the public records exception.[232] References to "widely distributed media" are common in the "government records plus" version of the public records exception.[233]

E. Step 3: The Notification

Data breach laws often contain a variety of notification provisions. For simplicity, this Article categorizes some of the major notification requirements as who, what, when, and how.

Who	Who must be notified?	Does the breach law also apply to government agencies and third parties?
What	What information must the notice include?	What type of injury is sufficient to require notice?
When	When must the notification be made?	When may notification be delayed?
How	How may the entity provide notice?	How does the data breach law interact with other laws?

Table 1. Major notification provisions

1. Who?

Consider the first question: who must be notified? There are three main recipients of data breach notifications: the consumer, the state Attorney General, and credit reporting agencies. State data breach laws always address notification to the data subject, as this is part of the laws' fundamental purpose. Thirty-two states require that notification also be submitted to the AG's office or other government

[231] *E.g.*, MINN. STAT. § 325E.61(1)(f) (2019).

[232] CONN. GEN. STAT. § 36a-701b (2019); DEL. CODE ANN. tit. 6, § 12B-101 (2019); IDAHO CODE § 28-51-104 (2019); IND. CODE § 24-4.9-2-10 (2019); IOWA CODE § 715C.1 (2019); ME. REV. STAT. ANN. tit. 10, § 1347 (2019); MD. CODE ANN., COM. LAW § 14-3501 (2018); MISS. CODE ANN. § 75-24-29 (2018); MO. ANN. STAT. § 407.1500; N.J. STAT. ANN. § 56:8-161; N.M. STAT. ANN. § 57-12C-2 (2019); N.C. GEN. STAT. § 75-61 (2018); OHIO REV. CODE ANN. § 1349.19 (West 2019); OK. STAT. tit. 24, § 162 (2019); S.C. CODE ANN. § 39-1-90 (2018); UTAH CODE ANN. § 13-44-102 (West 2019); VT. STAT. ANN. tit. 9, § 2430 (2019); VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-101 (2017); WIS. STAT. § 134.98 (2017); WYO. STAT. ANN. § 40-12-501 (2019). Michigan's language is unclear as to whether non-government documents are included. MICH. COMP. LAWS § 445.72 (2019) ("This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.").

[233] *E.g.*, CONN. GEN. STAT. § 36a-701b.

agency.[234] While most states allow the AG notification to be made at the same time as the notice to consumers, Maryland and New Jersey both require the AG to be notified before the consumers are notified.[235] Additionally, 36 states require credit reporting agencies to be notified, though the notice sent to the agencies may sometimes be required to omit specific information.[236]

The second question asks: who is bound by the requirements? The party most likely to be subject to the requirements is the data owner. Most of the data breach laws in the United States require third parties who maintain data owned by someone else to notify the data owner in the event of a breach, and then it will be the responsibility of the data owner to follow the notification requirements. Data owners are thus generally responsible for notifications, even if the data owner entered into an agreement with a third party to process or store some of its data.

In a minority of states, the data breach law appears to not apply to breaches of government systems. New Mexico is the only state that explicitly states that the data breach provisions do not apply to government agencies.[237] Most of the other laws

---

[234] ALA. CODE 8-19F-6 (2019); ARIZ. REV. STAT. ANN. § 18-552(B)(2)(b) (2019); CAL. CIV. CODE § 1798.82 (West 2019); COLO. REV. STAT. § 6-1-716(2)(f) (2019); CONN. GEN. STAT. § 36a-701b; DEL. CODE ANN. tit. 6, § 12B-102; FLA. STAT. § 501.171(3) (2019) (Department of Legal Affairs); HAW. REV. STAT. § 487N-2 (2019); IDAHO CODE § 28-51-105; 815 ILL. COMP. STAT. 530/12 (2019); IND. CODE § 24-4.9-3-1 (2019); IOWA CODE § 715C.2; LA. ADMIN. CODE tit. 16, § 701 (2015); ME. REV. STAT. ANN. tit. 10, § 1348; MD. CODE ANN., COM. LAW § 14-3504; MASS. GEN. LAWS ch. 93I, § 3 (2019); MO. ANN. STAT. § 407.1500; MONT. CODE ANN. § 30-14-1704 (2019); NEB. REV. STAT. § 87-803 (2019); N.H. REV. STAT. ANN. § 359-C:20 (2019); N.J. STAT. ANN. § 56:8-163; N.M. STAT. ANN. § 57-12C-10; N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); N.C. GEN. STAT. § 75-65; N.D. CENT. CODE § 51-30-02 (2019); OR. REV. STAT. § 646A.604; 11 R.I. GEN. LAWS § 11.49.3-4 (2019); S.C. CODE ANN. § 39-1-90; S.D. CODIFIED LAWS § 22-40-20 (2018); VT. STAT. ANN. tit. 9, § 2435 (2019); VA. CODE ANN. § 18.2-186.6; WASH. REV. CODE § 19.255.010 (2019).

[235] MD. CODE ANN., COM. LAW § 14-3504(h) (2018); N.J. STAT. ANN. § 56:8-163(c)(1) (West 2019).

[236] ALA. CODE § 8-38-7; ALASKA STAT. § 45.48.040 (2019); ARIZ. REV. STAT. ANN. § 18-552(B)(2); COLO. REV. STAT. § 6-1-716(2)(d); D.C. CODE § 28-3852 (2019); FLA. STAT. § 501.171, GA. CODE ANN. § 10-1-912(d) (2019); HAW. REV. STAT. § 487N-2(f); 815 ILL. COMP. STAT. 530/12; IND. CODE § 24-4.9-3-1; KANN. STAT. ANN. § 50-7a02; KY. REV. STAT. ANN. § 365.732 (West 2019); ME. REV. STAT. ANN. tit. 10, § 1348; MD. CODE ANN., COM. LAW § 14-3506; MASS. GEN. LAWS ch. 93I, § 3; MICH. COMP. LAWS § 445.72 (2019); MINN. STAT. § 325E.61; MO. ANN. STAT. § 407.1500; NEV. REV. STAT. § 603A.220 (2017); N.H. REV. STAT. ANN. § 359-C:20; N.J. STAT. ANN. § 56:8-163; N.M. STAT. ANN. § 57-12C-10; N.Y. GEN. BUS. LAW § 899-aa; N.C. GEN. STAT. § 75-65; OHIO REV. CODE ANN. § 1349.19; OR. REV. STAT. § 646A.604; 73 PA. STAT. § 2305 (2019); 11 R.I. GEN. LAWS § 11.49.3-4; S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-24; TENN. CODE § 47-18-2107 (2019); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2019); VT. STAT. ANN. tit. 9, § 2435; VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE ANN. § 46A-2A-102; WIS. STAT. § 134.98.

[237] N.M. STAT. ANN. § 57-12C-12.

in this category instead use language referencing business and exclude government agencies by implication. In Connecticut, there is a data breach law that applies to state contractors,[238] and the primary data breach law applies only to persons doing business in the state,[239] so breaches at the state agencies themselves seem to not be subject to either set of requirements. Some states that subject government agencies to the same notification requirements do so in a separate section specifically about government data breaches.[240]

2. What?

The first major "what" question: what must the notice include? Twenty-five states address this question.[241] Wisconsin does not list what must be included, but does say that a person who receives a notification of a data breach can submit a written request to learn what personal information was acquired.[242] This makes it clear that Wisconsin law does not require the notification to include details about the personal information acquired. Still, Wisconsin residents are likely to receive that information as part of a notification from an out of state business, because most states with content requirements do require information about the type of personal information acquired. New Mexico, for example, specifically requires information about what personal information was affected.[243] California's law also requires such information, and goes further than other data breach laws by providing a model notice in the statutory text.[244]

The second major "what" question concerns the injury caused by the breach. Commonly, a data breach law's notification requirements will not trigger in the absence of a certain type of risk or injury. The data breach laws of nine states are written broadly enough that the notification requirement appears to be triggered by the mere inclusion of personal information in a breach,[245] but most states require

---

[238] CONN. GEN. STAT. § 4e-70.

[239] *Id.* § 36a-701b.

[240] *E.g.*, MD. CODE ANN., STATE GOV'T § 10-1305; OHIO REV. CODE ANN. § 1347.12.

[241] ALA. CODE § 8-38-5; ARIZ. REV. STAT. ANN. § 18-552; CAL. CIV. CODE § 1798.82 (West 2019); COLO. REV. STAT. § 6-1-716; FLA. STAT. § 501.171(3); HAW. REV. STAT. § 487N-2; 815 ILL. COMP. STAT. 530/10; IOWA CODE § 715C.2; MD. CODE ANN., COM. LAW § 14-3504; MASS. GEN. LAWS ch. 93H, § 3; MICH. COMP. LAWS § 445.72; MINN. STAT. § 13.055 (applicable to breaches at government agencies); MO. ANN. STAT. § 407.1500; N.H. REV. STAT. ANN. § 359-C:20; N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa; N.C. GEN. STAT. § 75-65; OR. REV. STAT. § 646A.604(5); 11 R.I. GEN. LAWS § 11-49.3-4; VT. STAT. ANN. tit. 9, § 2435; VA. CODE ANN. § 18.2-186.6; WASH. REV. CODE § 19.255.010; W. VA. CODE ANN. § 46A-2A-102; WIS. STAT. § 134.98; WYO. STAT. ANN. § 40-12-502 (2019).

[242] WIS. STAT. § 134.98(3)(c).

[243] N.M. STAT. ANN. § 57-12C-7.

[244] CAL. CIV. CODE § 1798.82(d)(1).

[245] IOWA CODE § 715C.2; ME. REV. STAT. ANN. tit. 10, § 1348 (2019); MONT. CODE ANN. § 30-14-1704 (2019); NEV. REV. STAT. ANN. § 603A.220 (2017); N.Y. GEN. BUS. LAW § 899-

something more. In 13 states, the data holder must notify when the compromised information has or could result in identity theft or similar fraud affecting the data subject.[246] Some states use broader language. Eighteen breach notification laws are triggered when the breach creates a risk of harm for the data subject.[247] Most of the states that focus on harm look for a reasonable risk of harm. The requirement in Alabama, though, is triggered by a substantial risk of harm, and the requirement in South Carolina is triggered by a material risk of harm.[248] Michigan requires a risk of substantial loss or injury and also provides guidance for determining if this threshold is met.[249] Notification requirements in Arizona and Iowa are triggered based on the likelihood of financial harm specifically.[250] In Wyoming, a breach is defined as including an unauthorized data acquisition that "causes or is reasonably believed to cause loss or injury" to a state resident.[251] Fourteen states focus on the risk of misuse of the information rather than harm or identity theft.[252] Maine requires an investigation to consider the likelihood of misuse, but does not explicitly tie the concept of misuse to the notice requirement.[253]

---

aa; N.D. CENT. CODE ANN. § 51-30-02 (2019); TENN. CODE ANN. § 47-18-2107 (2019); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2019).

[246] IND. CODE § 24-4.9-3-1 (2019); KAN. STAT. ANN. § 50-7a01 (2018); KY. REV. STAT. ANN. § 365.732 (West 2019); MICH. COMP. LAWS § 445.72, MO. ANN. STAT. § 407.1500, N.M. STAT. ANN. § 57-12C-6 (requiring a "significant risk of identity theft or fraud"); OHIO REV. CODE ANN. § 1349.19 (West 2019) ("material risk"); OK. STAT. tit. 24, § 162 (2019); 11 R.I. GEN. LAWS § 11-49.3-4 ("significant risk"); UTAH CODE ANN. § 13-44-202 (West 2019); VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-101; WIS. STAT. § 134.98 ("material risk").

[247] ALA. CODE § 8-38-5 ("substantial harm"); ALASKA STAT. § 45.48.010 (2019); ARK. CODE ANN. § 4-110-105 (2019); CONN. GEN. STAT. § 36a-701b (2019); DEL. CODE ANN. tit. 6, § 12B-102 (2019); FLA. STAT. § 501.171(4) (2019); HAW. REV. STAT. § 487N-1 (2019) (addressed in definition of "security breach"); LA. STAT. ANN. § 3074; MICH. COMP. LAWS § 445.72 ("substantial loss or injury"); MISS. CODE ANN. § 75-24-29 (2018); MONT. CODE ANN. § 30-14-1704; N.C. GEN. STAT. § 75-61; OR. REV. STAT. § 646A.604(8) (2017); 73 PA. STAT. § 2302 (2019); S.C. CODE ANN. § 39-1-90 (2018); S.D. CODIFIED LAWS § 22-40-20 (2018); WASH. REV. CODE § 19.255.010 (2019).

[248] ALA. CODE § 8-38-4(a)(3); S.C. CODE ANN. § 39-1-90(A)–(D)(1).

[249] MICH. COMP. LAWS § 445.72(3).

[250] ARIZ. REV. STAT. ANN. § 18-552(J) (2019); IOWA CODE § 715C.2.6.

[251] WYO. STAT. ANN. § 40-12-501(a)(vii) (2019).

[252] COLO. REV. STAT. § 6-1-716 (2019); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-105 (2019); KAN. STAT. ANN. § 50-7a02 (2018); MD. CODE ANN., COM. LAW § 14-3504 (2018); ME. REV. STAT. ANN. tit. 10, § 1348(B) (2019); NEB. REV. STAT. § 87-803 (2019); N.H. REV. STAT. ANN. § 359-C:20 (2019); N.J. STAT. ANN. § 56:8-163 (considering whether misuse is "reasonably possible"); N.C. GEN. STAT. § 75-61; S.C. CODE ANN. § 39-1-90; UTAH CODE ANN. § 13-44-202; VT. STAT. ANN. tit. 9, § 2435(d)(1) (2019) ("reasonably possible"); WYO. STAT. ANN. § 40-12-502.

[253] ME. REV. STAT. ANN. tit. 10, § 1348(B).

These two questions illustrate the potential for conflict between state laws based on linguistic choices. Only 11 states require data owners to document instances where they determined that a notification was not required.[254] Wyoming's requirements seem to not be tied to risk or likelihood but to a reasonable belief that a loss or injury was caused. Data owners that do business in multiple states have many considerations. If they are concerned about the public relations implications from announcing a data breach, they may look to minimize the number of notifications sent out. It may not be in society's best interest if data owners only report breaches to the minimum extent required by law, and only 11 states require data owners to document cases where there was a breach, an investigation, and a conclusion that a notification was not required.[255]

A third "what" question concerns the format of the information. In most of the analyzed data breach laws, the definition of a breach is limited to electronic files. The language of the laws in 30 states refers only to electronic files.[256] Some of the other laws explicitly apply data breach language to other formats,[257] while others treat personal information differently depending on whether it is implicated by the data breach requirements or the sections governing records disposal.[258] This is a substantive issue that must be addressed in any federal data breach legislation or model law.

---

[254] ALA. CODE § 8-38-5(f) (2019); ALASKA STAT. § 45.48.010(c) (2019); FLA. STAT. § 501.171(4)(c) (2019); IOWA CODE § 715C.2(6); LA. STAT. ANN. § 3074(I); MD. CODE ANN., COM. LAW § 14-3504; MO. ANN. STAT. § 407.1500(5); N.J. STAT. ANN. § 56:8-163(a); OR. REV. STAT. § 646A.604(8) (2017); S.D. CODIFIED LAWS § 22-40-20 (2018); VT. STAT. ANN. tit. 9, § 2435(d)(1).

[255] ALA. CODE § 8-38-5(f); ALASKA STAT. § 45.48.010(c); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2.6; LA. STAT. ANN. § 51:3074(I); MD. CODE ANN., COM. LAW § 14-3504(b)(4); MO. ANN. STAT. § 407.1500.2(5); N.J. STAT. ANN. § 56:8-163(a); OR. REV. STAT. § 646A.604(7); S.D. CODIFIED LAWS § 22-40-20; VT. STAT. ANN. tit. 9, § 2435(d)(1).

[256] ALA. CODE § 8-38-2; ARK. CODE ANN. § 4-110-103 (2019); COLO. REV. STAT. § 6-1-716 (2019); CONN. GEN. STAT. § 36a-701b (2019); DEL. CODE ANN. tit. 6, § 12B-102 (2019); GA. CODE ANN. § 10-1-912 (2019); IDAHO CODE § 28-51-105; 815 ILL. COMP. STAT. 530/5 (2019); IND. CODE § 24-4.9-2-2 (2019); KAN. STAT. ANN. § 50-7a02; LA. STAT. ANN. § 3073; ME. REV. STAT. ANN. tit. 10, § 1347; MICH. COMP. LAWS § 445.63 (2019); MINN. STAT. § 325E.61 (2019); MISS. CODE ANN. § 75-24-29 (2018); MO. ANN. STAT. § 407.1500; NEB. REV. STAT. § 87-802; NEV. REV. STAT. § 603A.020 (2017); N.H. REV. STAT. ANN. § 359-C:19; N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); N.D. CENT. CODE § 51-30-01 (2019); OHIO REV. CODE ANN. § 1349.19 (West 2019); OK. STAT. tit. 24, § 162 (2019); OR. REV. STAT. § 646A.202(1)(a); S.D. CODIFIED LAWS § 22-40-19(1); TENN. CODE § 47-18-2107 (2019); TEX. BUS. & COM. CODE ANN. § 521.053 (West 2019); VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-101 (2017); WYO. STAT. ANN. § 40-12-501.

[257] *E.g.*, ALASKA STAT. § 45.48.090(1).

[258] *E.g.*, CAL. CIV. CODE § 1798.80 (West 2019).

3. When?

A failure to notify data subjects of a breach in a timely manner is generally considered to be a violation of a data breach law. Thirty-two of the data breach laws analyzed for this Article do not provide a specific timeframe, instead requiring the notice to be made without unreasonable delay.[259] Texas requires notifications to be sent "as quickly as possible," while New Hampshire uses the language "as soon as possible."[260] The unreasonable delay language is preferable to the latter two, because it allows for reasonableness considerations to be a factor in enforcement.

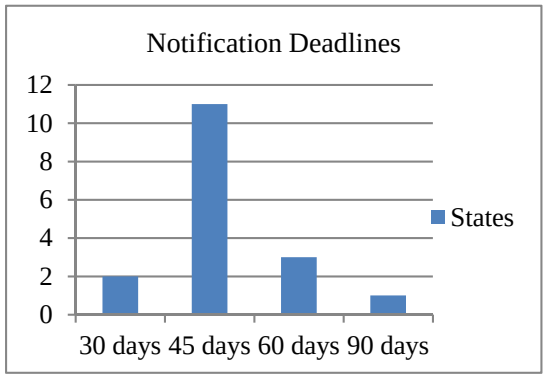

Figure 2. Deadlines for notification

The focus on unreasonable delays implies that there could be a reasonable delay. Forty-two of the analyzed laws include language suggesting that a reasonable delay would include time to recover from the breach.[261] This is commonly phrased to include time to determine the scope of the breach and time to restore system integrity. All of the analyzed data breach laws included explicit language allowing for delays due to a law enforcement investigation related to the breach.

---

[259] ALASKA STAT. § 45.48.010; ARK. CODE ANN. § 4-110-105; CAL. CIV. CODE § 1798.82(a); D.C. CODE 28-3852 (2019); GA. CODE ANN. § 10-1-912; HAW. REV. STAT. § 487N-2; IDAHO CODE § 28-51-105; 815 ILL. COMP. STAT. 530/10; IND. CODE § 24-4.9-3-3; IOWA CODE § 715C.2; KAN. STAT. ANN. § 50-7a02; KY. REV. STAT. ANN. § 365.732 (West 2019); ME. REV. STAT. ANN. tit. 10, § 1348; MICH. COMP. LAWS § 445.72; MINN. STAT. § 325E.61; MISS. CODE ANN. § 75-24-29; MO. ANN. STAT. § 407.1500; MONT. CODE ANN. § 30-14-1704 (2019); NEB. REV. STAT. § 87-803; NEV. REV. STAT. § 603A.220; N.J. STAT. ANN. § 56:8-163; N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65 (2018); N.D. CENT. CODE § 51-30-02; OK. STAT. tit. 24, § 163; 73 PA. STAT. § 2303 (2019); S.C. CODE ANN. § 39-1-90 (2018); UTAH CODE ANN. § 13-44-202 (West 2019); VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-102; WYO. STAT. ANN. § 40-12-502.

[260] N.H. REV. STAT. ANN. § 359-C:20(I)(a) (2019); TEX. BUS. & COM. CODE ANN. § 521.053.

[261] ALASKA STAT. § 45.48.010 (2019); ARK. CODE ANN. § 4-110-105; CAL. CIV. CODE § 1798.82; COLO. REV. STAT. § 6-1-716; CONN. GEN. STAT. § 36a-701b; D.C. CODE § 28-3852 (2019); FLA. STAT. § 501.171; GA. CODE ANN. § 10-1-912; HAW. REV. STAT. § 487N-2; IDAHO CODE § 28-51-105; 815 ILL. COMP. STAT. 530/10; IND. CODE § 24-4.9-3-3; IOWA CODE §

The "notification clock" for data breaches often starts running at the discovery of the breach. As noted above, 34 data breach laws use flexible language for notification deadlines, most commonly "without unreasonable delay."[262] The other 16 are divided across 30 days, 45 days, 60 days, and 90 days.[263] As the Figure 2 shows, 45 days is the most common deadline.

There are some states that require the data owner to investigate the data breach, and subsequent deadlines may be based on the date that investigation is completed. Maryland, for example, requires a "reasonable and prompt investigation."[264] The notification clock in Maryland starts upon completion of this investigation. Maryland is one of the states that does not use "without unreasonable delay" language, instead requiring that notices be sent within 45 days.[265] Some states reference investigations by the data owner without creating a formal requirement.[266]

4. How?

Data breach laws typically spend considerable space describing appropriate processes for notification. The type of notice permitted varies somewhat across different statutes. Primary means of notice generally include written notice, telephonic notice, and electronic notice that complies with the standards for electronic signatures and electronic records in 15 U.S.C. § 7001.[267]

715C.2; KAN. STAT. ANN. 50-7a02; KY. REV. STAT. ANN. § 365.732; LA. STAT. ANN. § 3074; ME. REV. STAT. ANN. tit. 10, § 1348; MD. CODE ANN., COM. LAW § 14-3504 (2018); MICH. COMP. LAWS § 445.72; MINN. STAT. § 325E.61; MISS. CODE ANN. § 75-24-29; MO. ANN. STAT. § 407.1500; MONT. CODE ANN. § 30-14-1704; NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. § 603.220; N.J. STAT. ANN. § 56:8-163; N.M. STAT. ANN. § 57-12C-9 (2019); N.Y. GEN. BUS. LAW § 899-aa; N.C. GEN. STAT. § 75-65; N.D. CENT. CODE § 51-30-02; OHIO REV. CODE ANN. § 1349.19; OK. STAT. tit. 24, § 163; OR. REV. STAT. § 646A.604; 73 PA. STAT. § 2303; S.C. CODE ANN. § 39-1-90; TEX. BUS. & COM. CODE ANN. § 521.053; UTAH CODE ANN. § 13-44-202(2); VT. STAT. ANN. tit. 9, § 2435 (2019); VA. CODE ANN. § 18.2-186.6; WASH. REV. CODE § 19.255.010 (2019); W. VA. CODE ANN. § 46A-2A-102; WYO. STAT. ANN. § 40-12-502.

[262] *Supra* notes 259–60.

[263] ALA. CODE § 8-38-5 (2019) (45 days); ARIZ. REV. STAT. ANN. § 18-552 (2019) (45 days); COLO. REV. STAT. § 6-1-716 (30 days); CONN. GEN. STAT. § 36a-701b (90 days); DEL. CODE ANN. tit. 6, § 12B-102 (2019) (60 days); FLA. STAT. § 501.171 (30 days); LA. STAT. ANN. § 3074 (60 days); MD. CODE ANN., COM. LAW § 14-3504 (45 days); N.M. STAT. ANN. § 57-12C-9 (45 days); OHIO REV. CODE ANN. § 1349.19 (45 days); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2) (2019) (45 days); S.D. CODIFIED LAWS § 22-40-20 (2018) (60 days); TENN. CODE § 47-18-2107 (2019) (45 days); VT. STAT. ANN. tit. 9, § 2435 (45 days); WASH. REV. CODE § 19.255.010 (45 days); WIS. STAT. § 134.98 (2017) (45 days).

[264] MD. CODE ANN., COM. LAW § 14-3504(b)(1).

[265] *Id.* § 14-3504(b)(3).

[266] *E.g.*, LA. STAT. ANN. § 3074(I); MISS. CODE ANN. § 75-24-29.

[267] *E.g.*, MD. CODE ANN., COM. LAW § 14-3504(e); N.J. STAT. ANN. § 56:8-163(c)(1) (West 2019).

Substitute notice methods generally become available when the cost of notifying affected individuals exceeds a threshold amount, when the number of individuals to be notified exceeds a threshold number, or when the data owner lacks sufficient contact information to provide notice. The dollar amounts that make a notification eligible for substitute notice range from $5,000 to $500,000.[268] The requirement for affected individuals ranges from 1,000 to 500,000, and some statutory language is ambiguous about whether that requirement is just for state residents or if the count of individuals to be notified includes all states. While the thresholds for substitute notice may not make a huge difference in the application of the laws, these broad ranges suggest that legislatures likely have different priorities when it comes to data breach notifications. Wyoming's law includes an explicit carve-out that lowers the substitute notice thresholds for Wyoming-based businesses.[269] This can either be interpreted as a recognition that in-state businesses are generally smaller businesses and need to have less burdensome options available for legal notice, or it might be a little bit of protectionism to favor Wyoming-based businesses over others since substitute notice is likely to be cheaper.

Substitute notice must generally include notice via email if the email address is known, conspicuous posting on the data owner's website, and notification to major statewide media. Florida is one of a few states where sending the notification to an email address, without reference to Section 7001, is considered a form of direct notice.[270]

Data owners would benefit from a consistent set of requirements. Thirty-nine of the data breach laws analyzed include language allowing data owners to use their own notification procedures if they are otherwise compliant. Consider a business that currently operates in a state that permits data owners to follow their own otherwise compliant procedures, like South Carolina.[271] The neighboring state of North Carolina does not include this language in its data breach law.[272] If a business wants to expand to North Carolina, it may have to evaluate and adjust its data breach practices. An important benefit of a federal data breach law is that it would standardize the process.

---

[268] *See, e.g.*, ALA. CODE § 8-38-5(e)(1); MISS. CODE ANN. § 75-24-29(6).

[269] WYO. STAT. ANN. § 40-12-502(d)(iii) (2019).

[270] FLA. STAT. § 501.171(4)(d) (2019).

[271] S.C. CODE ANN. § 39-1-90 (2018).

[272] N.C. GEN. STAT. § 75-65 (2018).

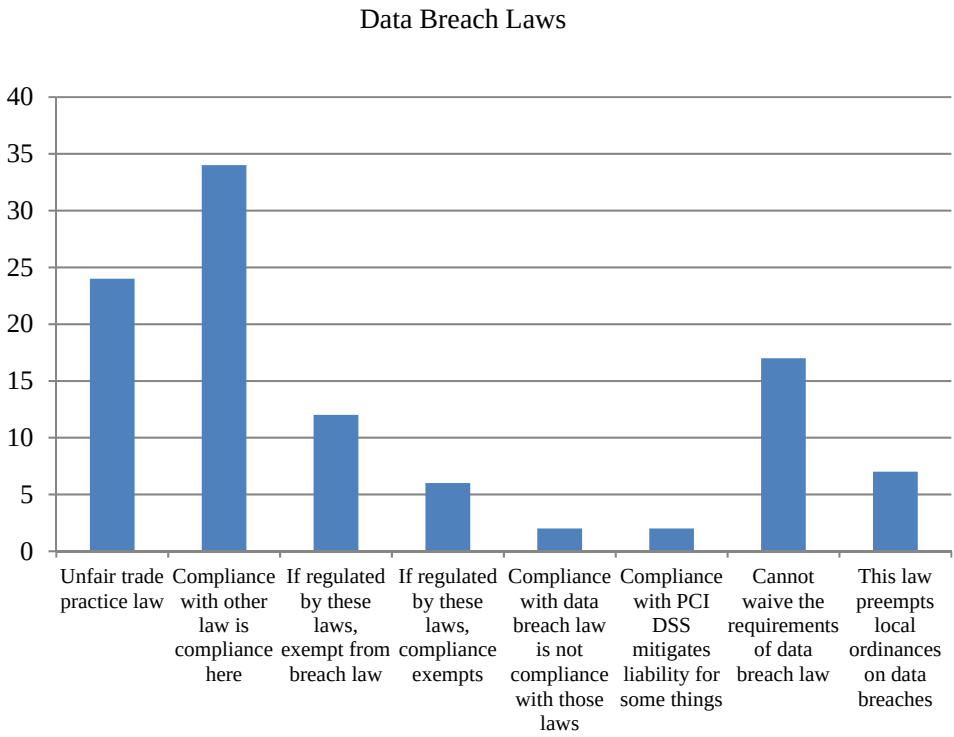

Figure 3: Interactions with other sources of legal obligations

Data breach laws also differ in how they address interactions with other laws. There are four major sources of law that data breach laws might address: consumer protection law, contract law, local law, and federal law. Twenty-four of the analyzed data breach statutes say that a violation of the data breach law is an unfair or deceptive act or an unlawful trade practice under state law.[273] Texas also references its deceptive trade practice law, but only for a violation of the prohibition on unauthorized possession or use of personal information.[274] Seventeen data breach laws

[273] ALA. CODE § 8-38-9; ALASKA STAT. § 45.48.080 (2019); ARIZ. REV. STAT. ANN. § 18-552 (2019); ARK. CODE ANN. § 4-110-108 (2019); CONN. GEN. STAT. § 36a-701b (2019); FLA. STAT. § 501.171(9); 815 ILL. COMP. STAT. 530/20 (2019); IND. CODE § 24-4.9-3-3.5 (2019) (deceptive act language only); IOWA CODE § 715C.2 (2019); LA. STAT. ANN. § 3074; MD. CODE ANN., COM. LAW § 14-3508 (2018); MASS. GEN. LAWS ch. 93H, § 6 (2019); MISS. CODE ANN. § 75-24-29; MONT. CODE ANN. § 30-14-1705 (2019); NEB. REV. STAT. § 87-806(2) (2019) (applying only to statutory security requirements); N.J. STAT. ANN. § 56:8-166; N.C. GEN. STAT. § 75-65 (requiring injury for deceptive act or practice); N.D. CENT. CODE § 51-30-07 (2019); OK. STAT. tit. 24, § 165 (2019); OR. REV. STAT. § 646A.604 (2017); 73 PA. STAT. § 2308 (2019); S.D. CODIFIED LAWS § 22-40-25 (2018); TENN. CODE § 47-18-2106 (2019); W. VA. CODE ANN. § 46A-2A-104 (2017).

[274] TEX. BUS. & COM. CODE ANN. § 521.051(a) (West 2019) ("A person may not obtain, possess, transfer, or use personal identifying information of another person without the other

emphasize that the requirements of the data breach law cannot be waived by contract,[275] and seven data breach laws explicitly state that the data breach law preempts local ordinances.[276]

Data breach laws vary on which federal laws or guidelines they address by name, but two common players are the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). The GLBA addresses data privacy issues affecting financial institutions and HIPAA concerns medical information.

Interaction with federal law and privacy standards gets a little linguistically sticky. Thirty-four data breach laws indicate that if the data owner is regulated by the specified laws, compliance with those laws counts as compliance with the data breach law.[277] In six data breach laws, the language indicates that entities are exempt from application of the law if they are regulated by and comply with other specified laws.[278]

---

person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name."); *id.* § 521.152 ("A violation of Section 521.051 is a deceptive trade practice actionable under Subchapter E, Chapter 17.").

[275] ALASKA STAT. § 45.48.060; ARK. CODE ANN. § 4-110-107; CAL. CIV. CODE § 1798.84 (West 2019); COLO. REV. STAT. § 6-1-716(2) (2019); D.C. CODE § 28-3852 (2019); HAW. REV. STAT. § 487N-2 (2019); 815 ILL. COMP. STAT. 530/15; MD. CODE ANN., COM. LAW § 14-3504; MINN. STAT. § 325E.61 (2019); NEB. REV. STAT. § 87-805; NEV. REV. STAT. § 603A.100 (2017); N.H. REV. STAT. ANN. § 359-C:21 (2019); N.C. GEN. STAT. § 75-65; OHIO REV. CODE ANN. § 1349.19 (West 2019); UTAH CODE ANN. § 13-44-202 (West 2019); VT. STAT. ANN. tit. 9, § 2435 (2019); WASH. REV. CODE § 19.255.010 (2019).

[276] ARIZ. REV. STAT. ANN. § 18-552; IND. CODE § 24-4.9-5-1; MD. CODE ANN., COM. LAW § 14-3505; MICH. COMP. LAWS § 445.72 (2019); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); 73 PA. STAT. § 2306; WIS. STAT. § 134.98 (2017).

[277] ARIZ. REV. STAT. ANN. § 18-552; ARK. CODE ANN. § 4-110-106; CAL. CIV. CODE § 1798.82; COLO. REV. STAT. § 6-1-716; CONN. GEN. STAT. § 36a-701b; D.C. CODE § 28-3852; DEL. CODE ANN. tit. 6, § 12B-103 (2019); FLA. STAT. § 501.171; HAW. REV. STAT. § 487N-2(g); IDAHO CODE § 28-51-106 (2019); 815 ILL. COMP. STAT. 530/45 (applicable to security requirements); *id.* 530/50 (HIPAA); IND. CODE § 24-4.9-3-4; KAN. STAT. ANN. § 50-7a02 (2018); LA. STAT. ANN. § 3076; ME. REV. STAT. ANN. tit. 10, § 1349 (2019); MD. CODE ANN., COM. LAW § 14-3507; MASS. GEN. LAWS ch. 93H, § 5; MICH. COMP. LAWS § 445.72; MISS. CODE ANN. § 75-24-29; MO. ANN. STAT. § 407.1500; NEB. REV. STAT. §§ 87-804 (notifications); *id.* 87-808 (security measures); NEV. REV. STAT. § 603A.210; N.H. REV. STAT. ANN. § 359-C:20; N.C. GEN. STAT. § 75-65; N.D. CENT. CODE § 51-30-06; OK. STAT. tit. 24, § 164; 73 PA. STAT. § 2307; 11 R.I. GEN. LAWS § 11-49.3-6(a)(1) (2019); S.C. CODE ANN. § 39-1-90 (2018); S.D. CODIFIED LAWS § 22-40-26; UTAH CODE ANN. § 13-44-202; VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-103; WYO. STAT. ANN. § 40-12-502 (2019).

[278] ALA. CODE § 8-38-11 (2019); IND. CODE § 24-4.9-3-3.5; IOWA CODE § 715C.2; OR. REV. STAT. § 646A.604; S.C. CODE ANN. § 39-1-90; WIS. STAT. § 134.98.

Twelve data breach laws use broader language that seemingly allows for an exemption from the data breach law just for being regulated by specified laws or entities.[279] Three of those, though, limit the exemption to the requirement to notify a credit report agency (CRA) about the breach.[280] The data breach laws of New Hampshire, West Virginia, and the District of Columbia say that the CRA notification requirement does not apply to entities regulated by Title V of the GLBA, which also addresses CRA notifications.[281] Similarly, California's exemption only applies to the provisions about data security.[282] These exemptions apply to entities regulated by California's Confidentiality of Medical Information Act, California's Financial Information Privacy Act, and HIPAA.[283] Outside of data security requirements, other references within California's law follow the more common "compliance there is compliance here" model.

Arkansas's law seems to provide a broad exemption, but it also includes conflicting language. In Section 4-110-106(a)(1), the law states:

> The provisions of this chapter do not apply to a person or business that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by this chapter.[284]

But then immediately following this broad "do not apply" language, the law immediately goes on in (a)(2): "Compliance with the state or federal law shall be deemed compliance with this chapter with regard to the subjects covered by this chapter."[285] This distinction between exemption and compliance creates ambiguity.

There are some other regulatory interactions considered in a minority of states. In Nevada and Washington, compliance with the Payment Card Industry Data Security Standards (PCI DSS) can mitigate some of a data owner's liability.[286] In both Maryland and Massachusetts, the data breach laws note that compliance is not transitive—that is, while compliance with another law might count as compliance with

---

[279] ALASKA STAT. § 45.48.040; ARIZ. REV. STAT. ANN. § 18-552; ARK. CODE ANN. § 4-110-106; CAL. CIV. CODE § 1798.81.5; D.C. CODE § 28-3852; KY. REV. STAT. ANN. § 365.732 (West 2019); N.H. REV. STAT. ANN. § 359-C:20; N.M. STAT. ANN. § 57-12C-8 (2019); OHIO REV. CODE ANN. § 1349.19; TENN. CODE § 47-18-2107 (2019); VT. STAT. ANN. tit. 9, § 2435; W. VA. CODE ANN. § 46A-2A-102.

[280] D.C. CODE § 28-3852(c); N.H. REV. STAT. ANN. § 359-C:20(VI)(b); W. VA. CODE § 46A-2A-102(f).

[281] D.C. CODE § 28-3852(c); N.H. REV. STAT. ANN. § 359-C:20(VI)(b); W. VA. CODE § 46A-2A-102(f).

[282] *See* CAL. CIV. CODE § 1798.81.5(e).

[283] *Id.*

[284] ARK. CODE ANN. § 4-110-106(a)(1).

[285] *Id.* § 4-110-106(a)(2).

[286] NEV. REV. STAT. § 603A.215 (2017); WASH. REV. CODE § 19.255.020 (2019).

the data breach law, compliance with the data breach law does not count as compliance with the other law.[287]

F. Step 4: Enforcement and Follow-Up

Enforcement of data breach laws varies widely. The previous Section noted that a lot of data breach laws reference state unfair trade practice laws in the context of enforcement. This simplifies matters for the state, because if a failure to notify is an unfair trade practice, no new legal process is needed because it fits into existing law. Again, though, this creates a variety of enforcement standards. Relying on unfair trade practice regulations to swallow data breach violations may also be inadvisable at a federal level because of resources. If a new breach law calls a notification violation an unfair trade practice, this indicates that much of the enforcement would be by the Federal Trade Commission (FTC), an agency that is increasingly being given responsibility for emerging data protection issues. Instead, perhaps a new office should be created to address data privacy and information technology regulatory issues.

In the analyzed data breach laws, the Attorneys General are often central players in enforcement, whether through authority over unfair trade practices or other sources of authority. Thirty-eight states and the District of Columbia assign the responsibilities of enforcement to the Attorney General.[288] Oregon takes a slightly

---

[287] MD. CODE ANN., COM. LAW § 14-3504(k) (2018) ("Compliance with this section does not relieve a business from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information."); MASS. GEN. LAWS ch. 93H, § 5 (2019) ("This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information. . . .").

[288] ALA. CODE § 8-38-9 (2019); ARIZ. REV. STAT. ANN. § 18-552; ARK. CODE ANN. § 4-110-108; COLO. REV. STAT. § 6-1-716(4) (2019) (generally); *id.* § 24-73-103 (for breaches at government agencies); CONN. GEN. STAT. § 36a-701b (2019); D.C. CODE § 28-3853 (2019); DEL. CODE ANN. tit. 6, § 12B-104 (2019); HAW. REV. STAT. § 487N-3 (2019); IDAHO CODE § 28-51-107 (2019); IND. CODE § 24-4.9-3-3.5 (2019); IOWA CODE § 715C.2 (2019); KAN. STAT. ANN. § 50-7a02 (2018); LA. STAT. ANN. § 3077; ME. REV. STAT. ANN. tit. 10, § 1349 (2019); MASS. GEN. LAWS ch. 93H, § 6; MICH. COMP. LAWS § 445.72 (2019); MINN. STAT. § 325E.61 (2019); MISS. CODE ANN. § 75-24-29 (2018); MO. ANN. STAT. § 407.1500; NEB. REV. STAT. § 87-806 (2019); NEV. REV. STAT. § 603A.290; N.H. REV. STAT. ANN. § 359-C:21 (2019); N.M. STAT. ANN. § 57-12C-11 (2019); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); N.C. GEN. STAT. § 75-9 (2018); N.D. CENT. CODE § 51-30-07 (2019); OHIO REV. CODE ANN. § 1349.19 (West 2019); OK. STAT. tit. 24, § 165 (2019); 73 PA. STAT. § 2308 (2019); 11 R.I. GEN. LAWS § 11-49.3-5(c) (2019); S.D. CODIFIED LAWS § 22-40-25 (2018); TENN. CODE § 47-18-2105 (2019); TEX. BUS. & COM. CODE ANN. § 521.151 (West 2019); UTAH CODE ANN. § 13-44-301 (West 2019); VT. STAT. ANN. tit. 9 (2019); § 2435, VA. CODE ANN. § 18.2-186.6; WASH. REV. CODE § 19.255.010; W. VA. CODE ANN. § 46A-2A-104 (2017); WYO. STAT. ANN. § 40-12-502 (2019).

different approach by giving authority directly to the Director of the Department of Consumer and Business Services.[289] Some of these provisions explicitly say that actions by the Attorney General are the exclusive method of enforcement.[290] Some of the laws state that no private action is created,[291] while others emphasize that no private action is lost.[292]

Data breach laws also frequently address whether individuals affected by a data breach can recover from the data owner. Ten data breach laws establish a private cause of action,[293] while other states make explicit that the data breach law does not create a private cause of action in at least some contexts.[294] Nevada is one of the states whose data breach law does not create a private cause of action.[295] However, Nevada does create a private cause of action for "data collectors" to recover notification costs from a party that obtained or benefited from the breached personal information.[296] This means that a cause of action is created for the party whose

---

[289] OR. REV. STAT. § 646A.624 (2017).

[290] *E.g.*, ALA. CODE § 8-38-9(a) ("The Attorney General shall have the exclusive authority to bring an action for civil penalties under this chapter."); ARIZ. REV. STAT. ANN. § 18-552(L) ("[O]nly the attorney general may enforce such a violation. . . ."); IND. CODE § 24-4.9-3-3.5 ("A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act that is actionable only by the attorney general under this section."); MO. ANN. STAT. § 407.1500.4 ("The attorney general shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section. . . ."); 73 PA. CONS. STAT. § 2308 (West 2019) ("The Office of Attorney General shall have exclusive authority to bring an action. . . ."); VT. STAT. ANN. tit. 9, § 2435 ("[T]he Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter. . . .").

[291] *E.g.*, MISS. CODE ANN. § 75-24-29(8) ("[N]othing in this section may be construed to create a private right of action."); NEB. REV. STAT. § 87-806(2) ("A violation of section 87-808 does not give rise to a private cause of action.").

[292] *E.g.*, VA. CODE ANN. § 18.2-186.6(I) ("Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section."); WYO. STAT. ANN § 40-12-502(f) ("The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.").

[293] CAL. CIV. CODE § 1798.84(b) (West 2019); D.C. CODE § 28-3853(a) (2019); HAW. REV. STAT. § 487N-1; KY. REV. STAT. ANN. § 365.730 (West 2019); LA. REV. STAT. § 51:3075 (2018); N.H. REV. STAT. § 359-C:21; N.C. GEN. STAT. § 75-65(i) (but only if the violation caused an injury to the person bringing the action); S.C. CODE ANN. § 39-1-90(G) (2018); TENN. CODE § 47-18-2105(a); WASH. REV. CODE § 19.255.010(13)(a).

[294] ALA. CODE § 8-38-9; FLA. STAT. § 501.171(10) (2019); IND. CODE § 24-4.9-3-3.5(e); NEV. REV. STAT. § 603A.360(3) (2017) (addressing lack of private action against operator); OHIO REV. CODE § 1349.192(A)(1) (West 2019); OK. STAT. tit. 24, § 165(B) (2019); 73 PA. STAT. §§ 2308 (2019); UTAH CODE § 13-44-201(2) (West 2019); WIS. STAT. § 134.98 (2017) ("Failure to comply with this section is not negligence or a breach of any duty").

[295] NEV. REV. STAT. § 603A.360.

[296] *Id.* § 270.

systems are breached, but not the data subject, raising the question of who should be seen as the "victim" of a data breach. The language of Wisconsin's law denies the creation of a new civil action, but says that violation of the notification provisions can be used as "evidence of negligence or a breach of a legal duty."[297]

Twenty-seven data breach laws address civil penalties.[298] In Louisiana's administrative code, the civil penalty for a violation of the notification provisions is $5,000.[299] Georgia mentions civil penalties, but the penalty appears to apply only to violations of the credit freeze provisions, so this may be superseded by recent changes to federal law.[300] Similarly, Massachusetts includes civil penalties, but only for violations of the records disposal law.[301] Washington State's data breach law does not address civil penalties, but it does highlight costs that the owner of the breached system may be required to pay.[302] In Washington, data processors that did not "take reasonable care to guard against unauthorized access" can also be required to reimburse financial institutions for the cost of reissuing credit and debit cards to affected data subjects.[303]

Advocates for a federal data breach law sometimes suggest including a requirement for a breached data owner to provide free credit monitoring. Such a policy is not yet widely adopted in the states. Connecticut is the only state that unambiguously requires free credit monitoring.[304] Delaware requires free credit monitoring to be offered, but only if social security numbers were compromised.[305] California's data breach law includes language requiring a minimum length of time when credit monitoring is offered, but there is an ambiguous "if any" in the middle of the provision: "If the person or business providing the notification was the source of the

---

[297] WIS. STAT. § 134.98(4).

[298] ALA. CODE § 8-38-9 (2019); ALASKA STAT. § 45.48.080 (2019); ARIZ. REV. STAT. ANN. § 18-552 (2019); CAL. CIV. CODE § 1798.84; D.C. CODE § 28-3853; FLA. STAT. § 501.171(9); HAW. REV. STAT. § 487N-3; IDAHO CODE § 28-51-107 (2019); IND. CODE § 24-4.9-3-3.5, 24-4.9-4-2; IOWA CODE § 715C.2.9.a (2019); LA. ADMIN. CODE tit. 16, § 701(b) (2015); ME. REV. STAT. ANN. tit. 10, § 1349 (2019); MICH. COMP. LAWS § 445.72 (2019); MO. ANN. STAT. § 407.1500; N.M. STAT. ANN. § 57-12C-11 (2019); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); OHIO REV. CODE ANN. § 1349.192; OK. STAT. tit. 24, § 165; OR. REV. STAT. § 646A.624 (2017); 11 R.I. GEN. LAWS § 11-49.3-5(b) (2019); S.C. CODE ANN. § 39-1-90; S.D. CODIFIED LAWS § 22-40-25 (2018); TENN. CODE § 47-18-2105; TEX. BUS. & COM. CODE ANN. § 521.151 (West 2019); UTAH CODE ANN. § 13-44-301(3); VA. CODE ANN. § 18.2-186.6; W. VA. CODE ANN. § 46A-2A-104 (2017).

[299] LA. ADMIN. CODE tit. 16, § 701(b).

[300] GA. CODE ANN. § 10-1-914.1(j)(1) (2019).

[301] MASS. GEN. LAWS ch. 93I, § 2 (2019).

[302] WASH. REV. CODE § 19.255.020(13) (2019).

[303] *Id.* § 19.255.020(3)(a).

[304] CONN. GEN. STAT. § 36a-701b(2)(B) (2019).

[305] DEL. CODE ANN. tit. 6, § 12B-102(e) (2019).

breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months."[306]

In Oregon, if a data owner offers credit monitoring services, the offer cannot be conditioned on the consumer providing a credit card number.[307] Additionally, Oregon law requires that any related paid services must be addressed separately from the free credit monitoring.[308] Montana's data breach law warns data owners that if they are going to tell data subjects about the breach and also inform the data subjects that they can contact CRAs, the data owners should let the CRAs know in advance.[309]

A few state data breach laws address general data practices as well. Nevada's data breach law includes language requiring transparency in online data collection.[310] Georgia, Maine, and Vermont also address the role of data brokers.[311] Companies that aggregate data play a prominent role in electronic commerce, and the inclusion of data brokers in a data breach law indicates an awareness of these dynamics and the potential threats to personal information. Colorado and Illinois both have data breach laws that prohibit data owners from passing off the cost of notification to the data subjects of the breach.[312]

G. Model Data Breach Laws

As noted elsewhere, the Uniform Law Commission is a major source for model legislation language. ULC formed a Data Breach Notification Committee (DBNC) in 2017,[313] and at the July 2018 Annual Meeting of the Committee on Scope and Program, the DBNC recommended that a model data breach law be drafted.[314] The Committee on Scope and Program did not approve the request, instead asking the DNBC to provide more information at the Committee's next midyear meeting in

---

306 CAL. CIV. CODE § 1798.82(d)(2)(G) (West 2019).

307 S. 1551, 79th Legis. Assemb., Reg. Sess., at 4 (Or. 2018).

308 *Id.*

309 MONT. CODE ANN. § 30-14-1704(7) (2019).

310 NEV. REV. STAT. 603A.340 (2017).

311 GA. CODE ANN. § 10-1-911(1) (2019) ("information broker"); ME. STAT. tit. 10, § 1347(3) (2018) ("information broker"); VT. STAT. ANN. tit. 9, § 2430(3) (2019) ("data collector").

312 COLO. REV. STAT. § 6-1-716(2)(a.5) (2019) ("A covered entity that is required to provide notice to affected Colorado residents pursuant to this subsection (2) is prohibited from charging the cost of providing such notice to such residents."); 815 ILL. COMP. STAT. 530/10(a) (2019) ("Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge . . . .").

313 ANNUAL MEETING OF THE COMMITTEE ON SCOPE AND PROGRAM, *supra* note 139.

314 *Id.*

January 2019.[315] In July 2019, the ULC authorized the creation of a drafting committee to focus on the collection and use of personally identifiable information.[316] ULC has thus shown interest in a uniform data breach law, but has not finalized a proposal. The American Law Institute (ALI) similarly has a current project examining data privacy, which has a tentative draft available.[317] The tentative draft was approved by ALI in 2019. It is unclear the extent to which data breach laws and model language will be addressed in the final version of this text.

Instead, this Article analyzes the model language provided by another outside drafter, ALEC. The ALEC proposal was first posted in 2006 and was most recently updated in 2012. ALEC's model data breach law includes 28 of the traits that were coded for in the larger study of data breach laws.[318] The following table lists these traits alongside how many enacted data breach statutes include similar or equivalent language.

Sample provision	Enacted	Sample provision	Enacted
Acquisition over time by the same entity counts as one breach	1	Approves of delays necessary to determine the scope of the breach and restore reasonable data integrity	43
This law preempts local ordinances on data breaches	7	Addresses interactions with other privacy laws that address breaches	45
Breach definition only covers threats to security and confidentiality, not integrity	8	Addresses electronic files only	46
Notification required when the stolen information has or could result in identity theft or fraud affecting information subject	13	Information in public records doesn't count as PII or accessing public records isn't a breach	48
Unauthorized access	16	Data breach law also applies to government agencies	48
Publicly available information, defined more broadly than public records	23	Good faith acquisitions by employees are not breaches	49
Violating statute's requirements is an unfair or deceptive act or unlawful trade practice	25	Unauthorized acquisition of data or PII	50

[315] *Id.*

[316] Katie Robinson, *New Drafting and Study Committees to be Appointed*, UNIF. L. COMM'N (July 24, 2019), https://www.uniformlaws.org/committees/community-home/digestviewer/viewthread?MessageKey=bc3e157b-399e-4490-9c5c-608ec5caabcc&CommunityKey=d4b8f588-4c2f-4db1-90e9-48b1184ca39a&tab=digestviewer.

[317] *Principles of the Law, Data Privacy*, AM. L. INST., https://www.ali.org/projects/show/data-privacy/ (last visited Jan. 19, 2020).

[318] *Breach of Personal Information Notification Act*, AM. LEG. EXCH. COUNCIL (amended June 23, 2017), https://www.alec.org/model-policy/the-breach-of-personal-information-notification-act/.

Sample provision (con't)	Enacted	Sample provision (con't)	Enacted
If the breach included the encryption key, you must disclose	27	Personal information is name PLUS something else	50
Civil penalties addressed in data breach law	29	Third party agents of covered entity experience a breach of data belonging to covered entity	50
Redaction and truncation	33	Financial account info PLUS means to access the account if needed (PIN, password, etc)	51
Entities regulated by other specified laws are deemed compliant with these requirements if they're compliant with their applicable laws	34	Encryption (e.g., PII definition excludes encrypted information, or notification is only required if the data was not encrypted)	51
Notification window starts at discovery of breach	37	Provision for delaying notice	51
You can use your own notification procedures if you're otherwise compliant	38	Law enforcement reasons to delay notification	51
AG can enforce data breach law	40	How to give notice	51

Table 2. Commonality of provisions in enacted legislation

As the table shows, most of the statutory traits noted in the ALEC model appear in a majority of enacted statutes. Many of these traits are described at high levels of generality. Readers are cautioned to avoid making assumptions about the influence of the model law based on these numbers, as it creates a chicken and egg problem. The current research identified 121 individual traits in data breach legislation, and ALEC's proposal contained only 28 of the "hard-coded" traits. ALEC's model also sides with eight states that omit risks to data integrity from the definition of a data breach, and 34 states that require notifications to be made without unreasonable delay. The ALEC model also joins five states and the District of Columbia by making substitute notice available when the cost of notification would exceed $50,000 or there are over 100,000 affected individuals.[319]

ALEC's accessibility increases its value as an example. Analyzing ALEC's model data breach language is instructive because it underscores many of the common threads across data breach laws. This Article's primary goal is to quantify some of these threads to enable the weaving of an efficient, unified data breach law.

[319] ARIZ. REV. STAT. ANN. § 18-552(F)(4) (2019); GA. CODE ANN. § 10-1-911(1)(D) (2019); OK. STAT. tit. 24, § 165(B) (2019); VA. CODE § 18.2-186.6(A)(4) (2019); W.V. CODE § 46A-2A-101(7)(D) (2019).

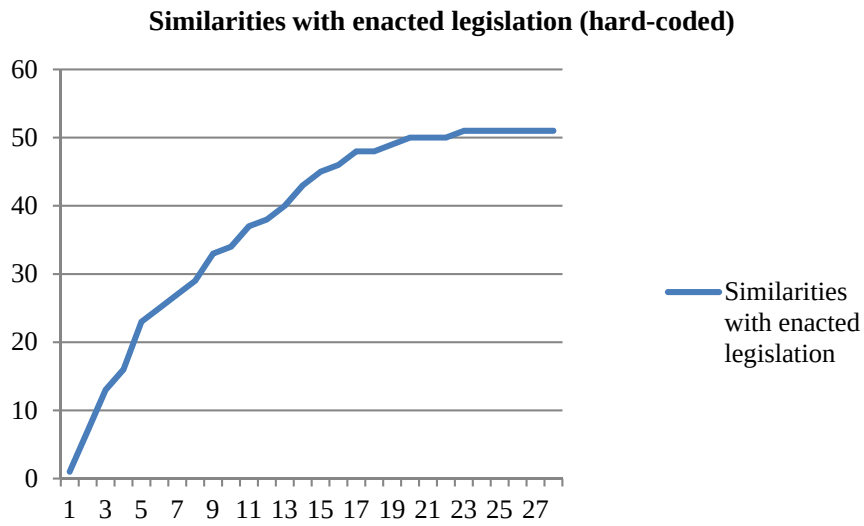

Figure 4. Similarities between ALEC proposal and enacted legislation

V. RECOMMENDATIONS

The above analysis empirically illustrates the range of approaches taken to data breach notification laws. There is a strong need for a uniform approach, which would reduce the inconsistency costs associated with having to comply with differing state laws.[320] Uniformity also reduces information costs for figuring out which law applies in which state, but this reduction of costs will likely only happen when the laws are almost totally uniform.[321] Uniformity can also mitigate some externalities that might otherwise result in a legislature ignoring activities that do not harm the state directly.[322]

This Section does not address every possible aspect of a unified data breach law. For example, sometimes state laws preempt local ordinances,[323] and this study found seven data breach laws with preemption provisions. The question of preemption is not something that this Article examines, but it will need to be considered in future legislative attempts.

Appendix A lists the 121 statutory traits identified in this study and organizes them into several groups.[324] These groups can be used to piece together a model

[320] Ribstein & Kobayashi, *supra* note 113, at 138.

[321] *Id.*

[322] *Id.* at 139.

[323] Snyder, *supra* note 26, at 416.

[324] *See infra* Appendix A Tables 1–4.

data breach law. This Section discusses recommendations for data breach law language based on several categories.

A. Prevention

A unifying data breach law should start with what this Article identified as Step One: Prevention. Data breach laws often include vague language requiring data holders to maintain reasonable data protections. Section IV.c. notes that Massachusetts and Oregon currently have the most detailed security requirements in their respective data breach laws. Massachusetts' approach to security is more technology focused,[325] whereas Oregon focuses on the proper structures being in place.[326] Because of the rapidly developing nature of technology, this Article supports a structural approach to security requirements.

Section 1 of Oregon's law reads:

> A person that owns, maintains or otherwise possesses data that includes a consumer's personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information.[327]

This Article favors the Oregon language because of its flexibility and structure. Another benefit of Oregon's law is that it simplifies the crossover between records disposal laws and data breach laws. Records disposal laws are often addressed separately from data breaches, creating opportunities for ambiguity and gaps in coverage.

Appropriate tools are also already available in NIST's Cybersecurity Framework (CSF).[328] The CSF is a voluntary framework initially proposed for critical infrastructure protection, but the principles of the framework are largely generalizable. The CSF uses a risk-based framework that is divided into five core functions: Identify, Protect, Detect, Respond, and Recover. Each function is subdivided into categories and subcategories.

The CSF is fundamentally about planning. The Identify core function emphasizes efforts to identify potential issues in advance. For example, Asset Management

---

[325] 201 MASS. CODE REGS. 17.04 (2018).

[326] OR. REV. STAT. § 646A.622 (2017) ("Requirement to develop safeguards for personal information . . . .").

[327] *Id.* § 646A.622(1).

[328] MATTHEW P. BARRETT, U.S. DEP'T COMM., VERSION 1.1, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 2 (2018), https://doi.org/10.6028/NIST.CSWP.04162018.

and Risk Assessment are two of the categories within the Identify core function.[329] The Protect core function is about prevention, and categories include Protective Technology and Maintenance. The Detect core function addresses steps to ensure that cybersecurity events are detected within a reasonable time. One category within the Detect core function is Security Continuous Monitoring. The Respond core function has categories that include Analysis and Mitigation. The Recover core function is about the resilience of systems, and Recovery Planning is one of its categories.

But what role should the CSF play? The two main options are for the data breach law to require compliance with the CSF, or for the law to consider compliance with the CSF when determining liability. The CSF is, at its core, a voluntary framework. Having a data breach law incorporate the CSF as a mandatory standard, therefore, would arguably be inconsistent with the way the framework is currently designed.

Nevada's data breach law provides an example and also an alternative formulation. Section 603A.215 of Nevada's law requires data collectors to comply with the Payment Card Industry Data Security Standards if they accept payment cards in the course of business.[330] For other data collectors, the law mandates that data must be encrypted if it is being moved or transmitted.[331] Compliance with the appropriate provision protects the data collector from liability for data breach damages, provided the data breach was not the result of gross negligence or intentional misconduct.[332]

While this Article does hold up Oregon's data breach law as a strong example for both structure and implementation, Nevada's law is only used as a structural model, because the implementation elements are inappropriate for a broader regime. The protections provided by Nevada's law are far too broad given how narrow the requirements are for data collectors not subject to the PCI DSS. Requiring that data be encrypted is a bare minimum as far as information security practices go and allowing encryption alone to outweigh any resulting data breach injury liability is an obvious thumb on the scale, disfavoring civil litigants. Nonetheless, the structure is instructive. Section 603A.215(3) reads:

> A data collector shall not be liable for damages for a breach of the security of the system data if:
>
> (a) The data collector is in compliance with this section; and
>
> (b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.[333]

---

[329] *Id.* at 7.

[330] NEV. REV. STAT. § 603A.215(1) (2017).

[331] *Id.* § 603A.215(2)(a).

[332] *Id.* § 603A.215(3).

[333] *Id.*

In line with the Nevada example, one option is to grant exemptions from liability if a data collector is in compliance with the CSF. An alternative is to use the CSF as a mitigating factor short of a liability exemption. If an audit shows that a data collector's practices are consistent with the CSF, for example, this documented compliance may weigh against a finding that the data collector did not use reasonable security practices. In that kind of model, security practices would not be sufficient to create a liability exemption, but they would be a factor to be considered in a flexible, case-by-case approach. This Article comes down on the side of flexibility rather than allowing compliance to provide a blanket exemption.

In the long run, cybersecurity policy may do well to imitate environmental policy. The Clean Air Act, for example, has some provisions which require polluters to adopt the best available control technology (BACT).[334] The broad, systemic effects of digital pollution are only starting to be understood. An analogous model might use a technology neutral "best available security technology" (BAST) standard.

B. Notifications

The notification aspects of a model data breach law should address several major questions: who must be notified, when must they be notified, and how?

The "who" question has several options: the consumer, the Attorney General, other government agencies, and credit reporting agencies. This can be further simplified as the individual, the regulator, and private entities. In terms of priority (if not chronology), the first party that will receive a notification is the affected consumer.

This Article has alternated between promoting a federal data breach law and a uniform data breach law. For a uniform law, state Attorneys General might remain the best avenue for regulatory oversight of data breaches, barring the existence of a more appropriate state agency. At the federal level, however, a more consumer-focused federal agency would almost always be a better regulatory choice than the Attorney General's office at the Department of Justice. Whether such a responsibility should be delegated to the Federal Trade Commission, the Consumer Financial Protection Bureau, or a new data-focused agency should be the target of future analysis.

This Article does not take a position on the degree to which private entities should be included in a data breach law. That question should be the subject of further analysis, including examination of base assumptions about why CRAs should be involved in the data breach reporting process at all. This is not to say that CRAs should be removed from discussions of data breaches, but this Article notes

[334] *Technology Transfer Network Clean Air Technology Center*, U.S. ENVTL. PROTECTION AGENCY, https://www3.epa.gov/ttncatc1/rblc/htm/welcome.html (last visited Oct. 20, 2019).

the possibility of removing that role as part of a restructuring of a systemic approach to data breaches.

Next is the "when." State data breach laws often favor a flexible "without unreasonable delay" standard, and this Article largely agrees with that approach. The language of data breach laws is currently inconsistent in terms of when a specific notification clock should start running. Say that a state requires a breached entity to notify victims of a breach within 60 days—but 60 days after what? One of the pervasive issues of cybersecurity policy is that an intrusion and breach often occur long before being discovered.

So Big Tech has a breach on January 1, and it discovers this on February 1. Big Tech conducts an investigation to determine the scope of the breach and identify the affected data. On March 1, Big Tech completes its investigation and now knows that there was a breach that compromised the security, confidentiality, and integrity of sensitive personal information. Obviously it would be unfair to start the 60-day notification limit on January 1, since Big Tech did not know about the breach until February 1. And if the data breach law only requires notifications when there was a compromise of the security, confidentiality, and integrity of personal information, then the notification requirement presumably would not be triggered until those things were known at some point between the discovery and the completion of the investigation. At the same time, though, a data breach law needs the right structure to prevent intentional foot-dragging that delays requirements.

This Article suggests using the popular "without unreasonable delay" model for data breach notifications, with an important modification: clarify which causes for delay are reasonable. In state data breach laws, this is typically done without much linguistic formality. In Section 1798.82(a) of California's law, for instance, the text reads: "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as proved in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[335]

A new data breach law should improve on existing models by explicitly setting forth examples of what factors may cause a delay to be reasonable. To this end, this Article proposes a three-part reasonableness standard for data breach notification delays. First, a delay is reasonable if it is necessary for law enforcement purposes. Further analysis would be beneficial for determining whether this should require an active investigation or, as in the discussion of obstruction of justice above, if a *de dicto* reading of "law enforcement purposes" would be more appropriate.

The second and third parts of the reasonableness standard focus on the data collector's investigation and system restoration. A delay should be considered reasonable if it is necessary to determine the scope of a data breach. This is important

[335] CAL. CIV. CODE § 1798.82 (West 2019).

because the scope determination is central to data breach notification obligations. A delay should also be considered reasonable if it is necessary to restore the integrity of the affected system. It is important to include recovery time within a reasonableness standard because unless system integrity is restored, a data breach cannot truly be said to be "over."

Finally, the "how." This question deserves more examination in future research, especially with insights from civil procedure. An examination of the processes and adequacy of legal notice is outside the scope of this Article, but the question of how to give meaningful notice is central for data breach policy. Examining data breach laws suggests a notice hierarchy, where email notice is often viewed as an inferior but necessary option.

Substitute notice, often defined to include widespread publication in addition to lower-ranked individual notification options like email, has an almost absurd range of thresholds. In New Hampshire, Mississippi, and Maine, substitute notice becomes available if the cost of notifications exceeds $5,000.[336] Alabama's new data breach law does not provide for substitute notice availability based on costs until projected notification costs exceed $500,000.[337] The presumably cheaper substitute notification options thus become available for breached entities at a much lower level in some states than in others.

Almost all data breach laws also say that a business can use slightly modified notification procedures as part of its internal security practices. Further research is needed to examine this element of data breach laws to see if it should be adopted in a more broadly applicable form. One benefit of allowing this kind of flexibility in state data breach laws is that companies that operate across state lines may have different requirements to meet in different states. The need for this flexibility diminishes with uniformity. Further analysis could examine whether the benefits of allowing modifications to enumerated procedures remains compelling when a statute has achieved uniformity.

Examinations of notice should also consider the content. Several state data breach laws list elements that should be included in a notification. Maryland, for example, requires a description of the affected categories of information, contact information for the business making the notification, contact information for both the FTC and the state Attorney General's office, and a statement referencing steps to prevent identity theft.[338]

This Article further asserts that a data breach law should require *meaningful* notice. Interdisciplinary work has special applicability because of the potential for behavioral insights into what makes a notice meaningful.

---

[336] ME. STAT. TIT. 10, § 1347(4)(c) (2018); MISS. CODE ANN. § 75-24-29(6) (2018); N.H. REV. STAT. ANN. § 359-C:20(III)(d) (2019).

[337] ALA. CODE § 8-38-5(e)(1)(a)(2) (2019).

[338] MD. CODE ANN., COM. LAW § 14-3504(g) (2018).

C. Enforcement

Enforcement of current data breach notification laws is currently inconsistent at best. Some states declare that only the state Attorney General's office has the authority to enforce the data breach law, while other states create a private cause of action. Data breach laws often, but not always, invoke consumer protection laws by reference.

A unified data breach law has a significant obstacle in front of it: the amorphous nature of data breach injuries. A solution will need to balance the high cost of lawsuits with the aggregated psychological and economic harms to countless individuals from data insecurity. One option that has been explored elsewhere is the possibility of a data breach compensation fund. Such a fund would provide a structure for accountability. In keeping with the metaphor of digital pollution, a unified data breach law could serve a role similar to CERCLA's Superfund Trust Fund. Fines could be used to compensate harmed individuals, but they could also be used for digital cleanup—that is, investments in security research.[339]

VI. CONCLUSION

Data breaches are a modern threat, and this Article has attempted to quantify some elements of policy responses to the threat. Language comprehension and statutory interpretation principles provide valuable context for the way that language shapes policy debates. Data breaches also lend themselves to analysis that considers extra-legislative origins of statutory text.

This Article empirically demonstrates that a unified data breach law is sorely needed. Such a law should focus on prevention, notification, and enforcement. A data breach law should require reasonable security practices and perhaps also adoption of the "best available security technology." The NIST Cybersecurity Framework can be applied to improve adoption of technology, though probably on a voluntary basis as an initial matter. A unified data breach law should focus on notification of the consumer and the regulator without unreasonable delay. Future research should examine the optimal role of credit report agencies in a data breach regime. Finally, a unified data breach law should have a mechanism for enforcement that ensures the protection of individual rights without imposing inefficiencies.

---

[339] *See* Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 360 (2019).

APPENDIX A: COLUMN HEADINGS

General information	Enforcement
State	Violating statute's requirements is an unfair or deceptive act or unlawful trade practice
Citation	State deceptive trade practice law citation if cited
Title	Notification violation does not create a private cause of action under unlawful trade practice law
Data breach law also applies to government agencies	Data breach law says private entities can be liable for economic damages under state unfair trade practices act
Law will expire	AG can enforce data breach law
Includes information brokers	Rulemaking authority relevant to data breaches addressed
Addresses electronic files only	Private cause of action for data breaches
Online data collection addressed	Private cause of action for breached data collector
Statutory organization	Remedy focused on compensating the breached data collector
First level	Civil penalties addressed in data breach law
Second level	Rights and remedies are cumulative with others available under the law
Second level redux	Regulating data collection

Appendix A Table 1. General information and enforcement

Notification requirements	
Notification window starts at discovery of breach	What information the notice must include
Notification window starts as of the conclusion of initial breach investigation	How to give notice
Notification required when the stolen information has or could result in identity theft or fraud affecting information subject	Substitute notice is okay if notification cost would exceed…
Notification required if their information was included in the breach	Substitute notice is OK if number of residents affected exceeds…
Notification required when there is a reasonable likelihood of financial harm	You can use your own notification procedures if you are otherwise compliant

Notification required when breach is likely to cause harm to information subjects	Document it anytime you decide that a notification is not required
Notification required if breach causes or is reasonably believed to cause injury or loss to state resident	Notify AG/government threshold
Notification required if misuse is reasonably possible	Notify AG timeframe
Notification required if misuse of personal information is reasonably likely	Notify consumer reporting agencies threshold
Notification must be made within what timeframe	Cannot delay notification because you need to notify consumer reporting agencies
Ask the AG for an extension if you cannot get it done by the deadline	Not required to tell the consumer reporting agency the breach victims' names or other PII
Reasonableness considerations	A court can order an entity to not issue a data breach notification
Provision for delaying notice	Companies cannot pass the cost of notification off on the customers
Law enforcement reasons to delay notification	If the security breach affected email login credentials, you cannot send the notice to that email if you provide the service
Approves of delays necessary to determine the scope of the breach and restore reasonable data integrity	Breach notification requirements do not require disclosure of trade secrets
When notifying, if you indicate to the recipients that they can get access to the information the consumer report agencies have on them, you have to coordinate with the consumer reporting agencies ahead of time	

Appendix A Table 2. Notification requirements

Security requirements	Personal information
Encryption (e.g., PII definition excludes encrypted information or notification is only required if the data was not encrypted)	Personal information is name plus something else
If the breach included the encryption key, you must disclose	Personal information includes name plus security token or shared secrets
Covered entities must implement reasonable security measures	Personal information might not include the name as long as what is there is enough for identity theft
Things to consider when assessing security system reasonableness	Personal information includes information that allows access to financial accounts regardless of whether a name is attached
Covered entities must ensure that third parties they send data to have reasonable security measures	Addresses personal information and PII separately

The state has detailed requirements for security practices	Financial account info plus means to access the account if needed (PIN, password, etc.)
Security measures should be appropriate for the nature of the data	Biometric data is PII for data breaches
Complying with security measures protects against liability for breach	DNA profile
Security measures requirements do not apply in some situations	Broad approach to PII
Records disposal	Information in public records does not count as PII or accessing public records is not a breach
Penalties available for improper record disposal	Publicly available information, defined more broadly than public records
At least some government agencies must have information security policies	The last four digits of account numbers are not personal information
Redaction and truncation	PII does not include information with extra conditions
Restrictions on how much of a credit card number can be on a receipt	Special callout for SSN

Appendix A Table 3. Security requirements and personal information

Breaches	Interaction with other laws	Miscellaneous (continued)
Define Breach	Addresses interactions with other privacy laws that address breaches	Breached entity must conduct investigation
Breach definition language	Entities regulated by other specified laws are exempt from these requirements	It is a crime to send out breach notifications when there was no breach (with intent to defraud)
Unauthorized acquisition of data or PII	Entities regulated by other specified laws are exempt from these requirements if they comply with their applicable law	Notifications to state enforcers are not public records, so there is no freedom to access them
Unauthorized access	Entities regulated by other specified laws are deemed compliant with these requirements if they are compliant with their applicable laws	Failure to comply may be evidence of negligence or breached duty
Unauthorized release	Compliance with data breach law does not count as compliance with those other laws	Who is responsible for the cost of reissuing credit and debit cards?
Unauthorized use	Compliance with PCI DSS is an exemption from liability for some things	Intentional improper disclosure by government employee is a crime
How to tell if there has been unauthorized acquisition	This law preempts local ordinances on data breaches	Breaches affecting government systems or information should be tracked and reported to the legislature or other government actors
Good faith acquisitions by employees are not breaches	Effect of similar federal statutes being enacted	Cannot waive the requirements of data breach law

It is not a breach for the government to get information with a court order or warrant		Government agencies should file annual reports about changes to personal information systems
Using information acquired because of a security breach is also a violation	Miscellaneous	Customers have the right to know when you sold their data to direct marketers
How to handle breaches affecting online accounts that might not be associated with a real name (e.g., separate provisions addressing online accounts and passwords)	Breached company must offer identity theft monitoring services	Data breach law does not apply in this specific regulated area
Third party agents of covered entity experience a breach of data belonging to covered entity	If you offer identity theft monitoring services for free, you cannot have certain conditions on the service	Out of state victims
Acquisition over time by the same entity counts as one breach	Industry specific breach laws	Data breach notice is not considered a debt notification
	References a government council about security and privacy	

Appendix A Table 4. Breaches, interaction with other laws, and miscellaneous

APPENDIX B: STATE DATA BREACH STATUTES

State	Statute Category	Citation
Alabama	Data Breaches	Ala. Code §§ 8-38-1 to 8-38-12
Alaska	Data Breaches	Alaska Stat. §§ 45.48.010 to 45.48.090
Arizona	Data Breaches	Ariz. Rev. Stat. §§ 18-551 to 18-552
Arkansas	Data Breaches	Ark. Code §§ 4-110-101 to 4-110-108
California	Data Breaches	Cal. Civ. Code §§ 1798.80 to 1798.84
	Data Breaches at Government Agencies	Cal. Civ. Code § 1798.29
	Medical Information	Cal. Health & Safety Code § 1280.15
Colorado	Data Breaches	Colo. Rev. Stat. § 6-1-716
	Data Breaches at Government Agencies	Colo. Rev. Stat. §§ 24–73–101 to 24-73-103
	Records Disposal	Colo. Rev. Stat. § 6-1-713
	Security Requirements	Colo. Rev. Stat. § 6-1-713.5
Connecticut	Data Breaches	Conn. Gen. Stat. § 36a-701b
Delaware	Data Breaches	Del. Code Ann. tit. 6 §§ 12B-101 to 12B-104
Florida	Data Breaches	Fla. Stat. § 501.171
	Unlawful Possession of Personal Information	Fla. Stat. § 817.5685

	Communication interception	Fla. Stat. § 934.03
Georgia	Data Breaches	Ga. Code §§ 10-1-910 to 10-1-915
	Computer Security	Ga. Code §§ 16-9-150 to 16-9-157
Hawaii	Data Breaches	Hawaii Rev. Stat. §§ 487N-1 to 487N-7
	Unlawful Possession of Personal Information	Hawaii Rev. Stat. § 708-839.55
Idaho	Data Breaches	Idaho Code §§ 28-51-104 to 28-51-107
Illinois	Data Breaches	Ill. Rev. Stat. ch. 815, 530/5 to 530/50
Indiana	Data Breaches	Ind. Code §§ 24-4.9-1-1 to 24-4.9-5-1
	Data Breaches at Government Agencies	Ind. Code §§ 4-1-11-1 to 4-1-11-10
Iowa	Data Breaches	Iowa Code §§ 715C.1 to 715C.2
Kansas	Data Breaches	Kan. Stat. Ann. §§ 50-7a01 to 50-7a04
Kentucky	Data Breaches	Ky. Rev. Stat. §§ 365.720 to 365.734
Louisiana	Data Breaches	La. Rev. Stat. §§ 51:3071 to 51:3077
	Reporting Requirements for Breaches	LA. ADMIN. CODE tit. 16, § 701
Maine	Data Breaches	Me. Rev. Stat. Ann. tit. 10, §§ 1346 to 1350-B
Maryland	Data Breaches	Md. Code, Com. Law §§ 14-3501 to 14-3508
	Data Breaches at Government Agencies	Md. Code, State Government, §§ 10-1301 to 10-1308
Massachusetts	Data Breaches	Mass. Gen. Laws 93H §§ 1 to 6
	Records Disposal	Mass. Gen. Laws 93I §§ 1 to 3
	Standards for the Protection of PII	201 MASS. CODE REGS. § 17.03
Michigan	Data Breaches	Mich. Comp. Laws § 445.72
Minnesota	Data Breaches	Minn. Stat. § 325E.61
	Data Breaches at Government Agencies	Minn. Stat. § 13.055
	Breach of Payment Data	Minn. Stat. § 325E.64
Mississippi	Data Breaches	Miss. Code § 75-24-29
Missouri	Data Breaches	Mo. Rev. Stat. § 407.1500
Montana	Data Breaches	Mont. Code Ann. § 30-14-1704
Nebraska	Data Breaches	Neb. Rev. Stat. §§ 87-801 to 87-808
Nevada	Data Breaches	Nev. Rev. Stat. §§ 603A.010 to 603A.290
New Hampshire	Data Breaches	N.H. Rev. Stat. §§ 359-C:19 to 359-C:21
	Medical Information	N.H. Rev. Stat. § 332-I:5
New Jersey	Data Breaches	N.J. Rev. Stat. §§ 56:8-161 to 56:8-166
New Mexico	Data Breaches	N.M. Stat. §§ 57-12C-1 to 57-12C-12
New York	Data Breaches	N.Y. Gen. Bus. § 899-aa

	Data Breaches at Government Agencies	McKinney's State Technology Law § 208
North Carolina	Data Breaches	N.C. Gen. Stat. § 75-65
	Records Disposal	N.C. Gen. Stat. § 75-64
North Dakota	Data Breaches	N.D. Cent. Code §§ 51-30-01 to 51-30-07
Ohio	Data Breaches	Ohio Rev. Code §§ 1349.19, 1349.191, 1349.192
	Data Breaches at Government Agencies	Ohio Rev. Code § 1347.12
Oklahoma	Data Breaches	Ok. Stat. tit. 24, §§ 161 to 166
Oregon	Data Breaches	Or. Rev. Stat. § 646A.604
	Data Protection	Or. Rev. Stat. § 646A.622
Pennsylvania	Data Breaches	73 Pa. Stat. §§ 2301 to 2329
Rhode Island	Data Breaches	R.I. Gen. Laws §§ 11-49.3-1 to 11-49.3-6
South Carolina	Data Breaches	S.C. Code Ann. § 39-1-90
	Data Breaches at Government Agencies	S.C. Code Ann. § 1-11-490
South Dakota	Data Breaches	S.D. Cod. Laws §§ 22-40-19 to 22-40-26
Tennessee	Data Breaches	Tenn. Code §§ 47-18-2105 to 2107
Texas	Data Breaches	Tex. Bus. & Com. Code § 521.053
	Data Breaches at Government Agencies	V.T.C.A., Government Code § 2054.1125
	Data Protection	Tex. Bus. & Com. Code § 521.052
Utah	Data Breaches	Utah Code §§ 13-44-101 to 13-44-301
Vermont	Data Breaches	Vt. Stat. Ann. tit. 9, §§ 2430 to 2447
Virginia	Data Breaches	Va. Code § 18.2-186.6
	Medical Information	Va. Code § 32.1-127.1:05
	Tax Information	Va. Code § 58.1-341.2
Washington	Data Breaches	Wash. Rev. Code §§ 19.255.010 and 19.255.020
West Virginia	Data Breaches	W.V. Code §§ 46A-2A-101 to 46A-2A-105
Wisconsin	Data Breaches	Wis. Stat. § 134.97 to 134.98
Wyoming	Data Breaches	Wyo. Stat. § 40-12-502