# RED, BLUE & PURPLE DATA BREACH LAWS: WHAT THEY REVEAL

*By: Chlotia Garrison, Clovia Hamilton, Danko Tarabar, Marguerite Doman, David Scibelli*[*]

ABSTRACT

The increase in data breaches is a serious threat to the protection of consumer information. Timely notification of the consumers' vulnerability after a breach is essential. Currently, in the U.S., no federal data breach notification law exists. Given the advancements of Artificial Intelligence (AI) and its potential for a greater and more critical role in our daily lives, the lack of federal breach legislation is of even greater concern. The issue for operating American businesses is that currently each state has their own law. Given the Internet of Things, and the fact that businesses have customers located in different states, without a federal law, businesses need to figure out each states' law and comply with each. Additionally, the multiple state laws with their varying requirements makes it burdensome for companies to comply. Addressing these concerns, this article reviews the U.S. data breach notification laws at the state level to inform the drafting of a much-needed federal law. We analyze the content of the laws considering when they were enacted, the definition of personal information, the notification deadline, and the regulatory strictness which we define as the combination of biometrics, restricted reporting deadlines, and health/medical information.

We hypothesized that: (1) the contents of the laws have changed from their original content, (2) there is a relationship between the contents of the law and when the original law was passed, and (3) one political party would dominate when the original law was passed. We found our first hypothesis to be true that the laws have changed content from their original passage. Approximately 70% of the state laws have been amended. Our research also supports our second hypothesis that

---

[*] Chlotia Garrison, PhD FL State University; Danko Tarabar, PhD West VA University; Marguerite Doman, PhD UNC Charlotte; and David Scibelli, DSc Robert Morris University; all of Winthrop University College of Business and Technology. Clovia Hamilton, PhD, JD faculty at the Indiana University Kelley School of Business. The authors wish to thank Dr. John Holden, JD of the Kelley School for his guidance.

a relationship exists between the contents of the law and when the initial data breach notification law was passed. An increase in the regulatory strictness of laws was discovered. This provides evidence of states' attempts to improve the content of these laws. Our third hypothesis was not supported. We found that purple states with joint control in the executive and legislative branches dominated when the original state data breach laws were enacted. This research is significant because it provides evidence that although there is a patchwork of state policies, there exist commonalities in the state laws that could be used to draft a bipartisan federal law. This federal law should be accomplished with bipartisan dialogue in the U.S. Congress. A model code created by the Uniform Law Commission (ULC) would not suffice because of the long timeframe it takes for the ULC to promulgate uniform model codes. Given the rapid advancement of AI threats to data protection, there is no time to waste. A federal law would ease the burden on companies that must accommodate the multiple provisions of multiple state laws.

**Keywords:** data breach, data breach notification, data protection, personal information, artificial intelligence, AI, AI ethics, AI threats, GDRP, CCPA, privacy, cybersecurity

I. INTRODUCTION ..... 158
II. CHARACTERISTICS OF INTERNATIONAL APPROACHES TO DATA BREACH LAWS ..... 160
*A. European Union's General Data Protection Regulation* ..... 160
*B. Characteristics of data protections in Asia* ..... 163
III. DATA PROTECTIONS IN THE USA ..... 166
*A. California Consumer Privacy Act* ..... 166
*B. Efforts in US Federal Legislation* ..... 168
*C. Artificial Intelligence advancement promotes urgency for a U.S. federal law* ..... 171
IV. CHARACTERISTICS OF THE LAST ENACTED US STATE LAWS ..... 176
*A. Definition of Security/Data Breaches* ..... 177
*B. Definition of Personal Information* ..... 177
*C. Notice Deadlines and Exceptions* ..... 179
*D. Methods of Delivering Notices of Data Breaches* ..... 179
*E. Required Minimum Content of the Notification* ..... 180
*F. Penalties* ..... 180
V. METHODOLOGY ..... 181
VI. RESULTS ..... 184
*A. Content Analysis* ..... 184
1. Legislation Timeline ..... 184
3. Definition of Personal Information ..... 185
a. Biometric Data ..... 185
b. Health Data ..... 189
4. Restricted Notification Deadline ..... 191
5. Additional characteristics ..... 194
*B. Statistical Analysis* ..... 195
VII. BUSINESS IMPLICATIONS ..... 206
VIII. CONCLUSION ..... 207
APPENDIX ..... 211

## I. INTRODUCTION

Hackers stole the personal data of 57 million Uber customers, yet Uber did not disclose the breach for a year.[1] The hackers wanted $100,000 to delete their copy of the data and Uber made the payment.[2] Uber also fired its security executive.[3] In 2022, Uber's security executive was on trial for obstructing justice for failing to disclose the breach.[4] According to Kyung-shick Choi, Director of Metropolitan College's Cybercrime Investigation & Cybersecurity programs, the harm to customers is that the personal data "can be weaponized and used against them" to gain finances, take over accounts, and for other criminal purposes.[5] Also, in 2022, an 18-year-old hacked Uber to illustrate how weak their security system was and demanded that Uber drivers get higher pay.[6] The hacker posed as an information technology worker and convinced an Uber contractor to divulge his password to Uber's systems. Using the password, the hacker logged in and bypassed Uber's two-factor log-in authentication.[7]In another breach, it took Equifax forty-one days to notify the public of a data breach that was originally reported to have exposed the data of 143 million people. This estimate was later increased to 145.5 million.[8] The increase in security or data breaches is a serious threat to the protection of consumer information. Timely notification of the consumers' vulnerability after a breach is essential. There were more data breaches in 2021 than in any year since 2003 when the first states began requiring breaches to be reported.[9] The year 2022 saw the second highest number of data breaches.[10]

In the second half of 2005 a significant increase in data breaches exposed more than a million records. One hundred thirty-six data

---

1. Andy Greenberg, *Hack Brief: Uber Paid Off Hackers to Hide A 57-Million User Data Breach*, WIRED (Nov. 21, 2017, 7:56 PM), https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/.

2. Kate Conger & Kevin Roose, *Uber Investigating Breach of its Computer Systems*, N.Y. TIMES (Sep 15. 2022), https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html.

3. *Id.*

4. *Id.*

5. Lindsay Shachnow, *Uber Users: What You Need to Know About Last Month's Data Breach*, BU TODAY (Oct. 11, 2022), https://www.bu.edu/articles/2022/what-you-need-to-know-about-uber-data-breach/.

6. Conger & Roose, *supra* note 2.

7. Shachnow, *supra* note 5.

8. Alex Johnson, *Equifax Breaks Down Just How Bad Last Year's Data Breach Was*, NBC NEWS (May 8, 2018, 6:25 PM), https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496.

9. *Identity Theft Resource Center 2021 Annual Report* (2021), IDENTIFY THEFT RES. CTR. (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

10. *Identity Theft Resource Center 2022 Data Breach Report (2022)*, IDENTITY THEFT RES. CTR. (Jan. 2023), https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/.

breaches occurred in 2005, impacting 60.3 million records.[11] In response to these data breaches several states passed data breach notification laws. Over a ten-year period, 2009 to 2018, a total of 7,988 data breaches occurred.[12]

Currently, in the United States of America, no federal data breach notification law exists. Individual state data breach notification laws vary. In addition, multiple federal agencies have added sector-specific reporting requirements that also vary.[13] Therefore, when a data breach occurs, companies must consider each individual U.S. state data breach notification law that applies to their customers. The state statutes vary regarding breach notifications and management, making it difficult to navigate this patchwork of legislation. Further, the acquisition or merger of companies potentially requires learning and adhering to a new set of state laws when geographical boundaries change. In addition, companies must consider the past data breaches experienced by companies and their related financial obligations, damaged reputation, and any required monitoring and reporting obligations. Based on these concerns, this article provides a review of the U.S. data breach notification laws at the state level. We analyze the content of the laws at the time they were enacted, the definition of personal information, the notification deadline, and the regulatory strictness which we define as the combination of biometrics, restricted reporting deadlines, and health/medical information. This review can also help inform the contents of a federal data breach notification law and help companies determine the minimum requirements following a data breach.

Part II of this paper provides characteristics of international approaches to data breach laws. This includes a discussion of the European Union's General Data Protection Regulation (GDPR) and characteristics of data protections in Asia. We lead with a discussion of international approaches to data breach laws because given the Internet of Things (IoT) and how global business is today, businesses no longer operate in their country's silos. It behooves business leaders to understand international laws. To this end, we chose to explain the European Union's and Asia's approaches to data breach protection.

Part III discusses data protections in the U.S. The U.S. discussion includes information about the California Consumer Privacy Act, efforts to enact federal legislation, and how the advancement of artificial

---

11. Privacy Rights Clearinghouse, *Data Breaches* (2018), https://www.privacyrights.org/data-breaches.

12. Anu Petrosyan, *Annual Number of Data Compromises and Individuals Impacted in the United States From 2005 to 2023*, STATISTA (Dec. 10, 2024), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed.

13. Scott Ferber et al., *Federal Data Breach Reporting Requirements Continue to Evolve*, XII NAT'L L. REV. (Dec. 9, 2021), https://natlawreview.com/article/federal-data-breach-reporting-requirements-continue-to-evolve#google_vignette.

intelligence (AI) has created an urgency for a U.S. federal law. Part IV provides characteristics of the last enacted U.S. state laws. This discussion includes these states' definitions of security and data breaches and personal information. It also includes the states' data breach notice deadlines and exceptions; methods of delivering notices of data breaches; the required minimum content of these notices; and penalties for noncompliance. Regarding personal information, we analyzed the regulatory strictness which we define as the combination of biometrics, restricted reporting deadlines, and health/medical information.

Part V includes a general discussion of the U.S. state data breach notification statutes and explains the empirical and statistical method used to analyze the data breach notification laws for this research study. Part VI provides the study findings. This includes information about the state legislation timelines; how states have amended their data breach legislation; changes in the definitions of personal information; restricted data breach notification deadlines and other characteristics in these data breach statutes. There is also a statistical analysis of the state data breach laws; and an analysis of the legislative and executive branch leaders' political affiliations at the time these laws were enacted. Part VII provides implications for business managers and owners; and Part VIII provides our conclusions.

## II. CHARACTERISTICS OF INTERNATIONAL APPROACHES TO DATA BREACH LAWS

### *A. European Union's General Data Protection Regulation*

The European Union (EU) has addressed the problem of privacy with data protection regulation including breach notification to protect consumers and their data within all its members.[14] The GDPR was passed by the EU Parliament on April 27, 2016. It became effective on May 25, 2018.[15] Major components of the GDPR include: (1) application to all entities that process the personal data of EU residents even if the company is not an EU entity;[16] (2) breach notification must be done within 72 hours;[17] (3) tiered penalties up to the larger of four percent (4%) of the previous annual revenue or 20 million Euro, approximately

14. Fredric Bellamy, *Cybersecurity Legal Compliance Update: Spring 2018 Brings Sea Change to Data Breach Notification Laws,* LEXOLOGY (June. 6, 2018), https://www.lexology.com/library/detail.aspx?g=6ad66252-79f8-4ab6-a54d-4bcd5fbcd24c.

15. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

16. *See id.* at pmbl. 78; *id.* at ch.1, art.2(1), art.3.

17. *See id.* at pmbl. 85; *see id.* at ch. IV, § 2, art. 33.

$23.5 million;[18] (4) that consent must be clear, distinguishable from other issues, provided in clear and plain language void of formal legal language[19] and easy to give and withdraw;[20] (5) individuals have the right to know about, and obtain an electric copy of, any personal data being processed and be able to obtain an electronic copy of it;[21] (6) individuals have the right to have their data erased;[22] (7) individuals can access and transmit their data to other entities;[23] (8) entities must design the protection of personal information into their system;[24] and (9) member states require internal record keeping requirements for certain entities.[25]

In May 2018, as a result of the new EU requirements, international companies began notifying their customers of changes to their privacy policies. Consumers began receiving notices of updated privacy statements by email and as they logged into their existing online accounts.[26] A sample of such an email follows:

> *Because you are a valued Ready Hosting customer, we want to let you know about upcoming changes to our Privacy Policy. If you are located in the European Union, these changes will go into effect for you as of May 23, 2018. If you are located outside of the European Union, these changes will go into effect for you as of June 23, 2018.*
>
> *We are making these changes to better explain our privacy practices to you and to reflect changes required by the European General Data Protection Regulation (GDPR). This includes core information about how we collect, use, and share any personal information you may give to us. We have reworded some content and added details with the objective of making our practices easy for our customers to understand.*
>
> *Notable updates include:*
>
> - *Greater Transparency. The new policy will provide more detailed explanations of what personal*

18. *Id.* at ch. VIII, art. 83(5).
19. *Id.* at pmbl. 32; and ch. II, art. 7.
20. *Id.* at pmbl. 42; and ch. II, art. 7.
21. *Id.* at ch. III, § 2, art. 13(1)(f); § 2, art. 15(3-4); and § 3, art. 17(2).
22. *Id.* at ch. III, § 3, art. 17(1).
23. *Id.* at pmbl. 68.
24. *Id.* at ch. IV, § 2, art. 32(1)(b).
25. *Id.* at pmbl. 19; and ch. II, art. 6(2).
26. Russell Brandom, *Everything You Need to Know About GDPR: GDPR Gives Companies a New Set of Rules for Sharing Data Online*, THE VERGE (May 25, 2018, 8:52 AM), https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice.

> *information we collect from you, how we collect it, what we do with it, and who we share your data with, including how we share information with advertisers and third parties.*
> - *More Control. We have new settings that will give you more choices about how you may share and control the information you give to us. The new policy will also outline specific procedures for asking us to stop or limit using the data we have about you*.[27]

The European Data Protection Board (EDPB) stated that the application of the EU General Data Protection Regulation had been successful in its first five- and one-half years (May 2018 to Dec 2023). Consumers are more aware of their privacy rights and companies are more aware of their obligations.[28]

Prior to the GDPR, all the member states had instituted their own data protection legislation in response to the EU's 1995 Data Protection Directive 95/46/EC. The 1995 Directive required the member states to protect the processing and free movement of personal data.[29] The GDPR provided needed unification of the individual member state laws.

The GDPR has served as an example and catalyst for other countries to implement privacy standards. Over 100 countries have put in place privacy standards.[30] For example, Australia has had a privacy act since 1988 but has amended its privacy act to reflect some GDPR regulations.[31] That act was amended in 2018 to add the notification of data breaches and again in 2022 to add enforcement and other measures.[32] The next section reviews characteristics of data protections in Asia.

---

27. Posting of ReadyHosting, info@e.readyhosting.com, to garrisonc@winthrop.edu (May 17, 2018) (on file with author).

28. European Data Prot. Bd., *Contribution of the EDPB to the Report on the Application of the GDPR Under Article 97*, at 3 (Dec. 15, 2023), https://www.edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-report-application-gdpr-under-article-97-2023_en.

29. European Union, EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on The Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation),2016 O.J. (L 119) 1; *see also* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2016).

30. Anthony Jones, *GDPR Three Years Later: What Impact Has It Made?*, I.S. PARTNERS, LLC (Aug. 16, 2022), https://www.ispartnersllc.com/blog/gdpr-one-year-later-impact/.

31. *Id.*

32. *History of the Privacy Act*, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER , https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act (last visited Jan. 25, 2025).

### *B. Characteristics of data protections in Asia*

U.S. and European businesses do not operate in a vacuum. Many are quite dependent on China for product manufacturing. The COVID-19 pandemic and related supply chain disruptions revealed how vulnerable that dependency is. While China will remain a very important trading partner, western businesses are looking for alternative manufacturing locations.[33] In Asia, businesses can look to the U.S.'s fourth largest trading partner, the Association of Southeast Asian Nations (ASEAN). ASEAN includes ten member countries: Thailand, Indonesia, Philippines, Vietnam, Burma, Cambodia, Singapore, Brunei, Laos, and Malaysia. The U.S. also has alliances with South Korea.[34] Doing business in Asia requires knowledge of Asian data protection laws. Thus, we provide examples of research related to recent regulations.

The challenges and opportunities of implementing personal data protection (PDP) in Indonesia have been researched. The researchers argue that the implementation of the Indonesian PDP Law of 2016 has been hampered by Indonesians' lack of awareness of their rights under the law and risks associated with the collection and processing of their personal data. Further, the Indonesian government lacks adequate resources to effectively enforce the law. Enforcement has been weak and has lacked coordination. Thus, there is a need to raise awareness and strengthen resources to improve regulatory enforcement.[35] In October 2022, the PDP Law of 2016 was amended to add a requirement for data controllers to conduct data protection impact assessments (DPIAs) and to establish a Data Protection Authority (DPA) to promote and enforce the law.[36]

The Japanese personal information protection system was established under a law called the Act on the Protection of Personal Information (APPI), which was enacted in 2003. The law provides a framework for the collection, use and disclosure of personal information by organizations. It gives individuals the right to access their personal information and the right to object to its processing. In 2017, in response to the increasing use of personal information by organizations and an increase in data breaches, amendments were made to the law. Under the amended law, organizations are to obtain consent from individuals before collecting their personal information. This researcher calls for

---

33. Clovia Hamilton, *Identifying Sources of Covid19 Pandemic Supply Chain Fragility*, AM. SOC'Y ENG'G MGMT. (ASEM) INT'L ANN. CONF. 1, 5–6 (2021).

34. *See* Richard Stubbs, *ASEAN PLUS THREE Emerging East Asian Regionalism?*, 42(3) ASIAN SURVEY 440, 440, 442 (2002).

35. *See* Diana Setiawati, Hary Abdul Hakim & Fahmi Adam Hasby Yoga, *Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore*, 2(2) INDON. COMP. L. REV. 95-109(2020).

36. *The New Era for Personal Data Protection in Indonesia,* PRICE WATERHOUSE COOPER, INDON., (Jan. 2023) at 3–4 , https://www.pwc.com/id/en/publications/legal/legal-alert-2023-14.pdf.

increased public awareness of the APPI and the importance of protecting personal information.[37]

Some researchers discuss the different perspectives of private sector stakeholders on the issues of mandatory data breach notification in Hong Kong. These researchers note that the primary objective of data breach notification laws is to regulate organizations' data security practices to provide customer data privacy protection. The authors interviewed twenty-four private sector representatives with interest in data breach issues to document and examine their position on the appropriate regulatory approach for data breach notification in Hong Kong. These researchers found that there is no consensus among the stakeholders on the issue of mandatory data breach notification. Some stakeholders supported mandatory notification, arguing that it is necessary to protect the privacy of data subjects and to promote accountability and transparency among organizations. Others opposed mandatory notification, arguing that it would be too costly and burdensome for organizations, and it could lead to false positives and unnecessary panic among data subjects. Ong & Sabapathy advocate that the government should carefully consider the views of all stakeholders before deciding on the regulatory approach for data breach notification.[38]

South Korea has been a frequent target of cyberattacks including attacks from North Korea. The National Cybersecurity Center (NCSC) is the government agency responsible for coordinating cybersecurity efforts in South Korea. The NCSC develops cybersecurity policies, regulations, and standards. It also monitors and responds to cybersecurity incidents and promotes cybersecurity public awareness. Regulations include the National Intelligence Service Act (NIS Act), the Cybersecurity Business Regulations, and the National Cyber Safety Management Regulations. The NIS Act gives the National Intelligence service (NIS) the lead role in coordinating the cybersecurity efforts.[39] Research uncovers that there have been few cases prosecuted by the NCSC, the definition of cybersecurity is not clear, the duties of the government agencies are not clear, and the NCSC lacks resources. These researchers recommend a

37. Kaori Ishii, *Advancements in the personal information protection system*, 1(3) GLOB. PRIV. L. REV. 164, 164-65, 172 (2020).

38. Rebecca Ong & Sandy Sabapathy, *Hong Kong's Data Breach Notification Scheme: From the Stakeholders' Perspectives*, 42 COMPUT. L. AND SEC. REV. 105579 (2021).

39. *See generally* Kwang Bae Park, Sunghee Chae & Hyein Lee, *Korea's Cybersecurity Regulations and Enforcement Related to Security Incidents*, 2(1) INT'L CYBERSECURITY L. REV. 47 (2021); Evan A. Feigenbaum & Michael R. Nelson, *Korea's Path to Digital Leadership: How Seoul CanLed on Standards and Standardization*, CARNEGIE ENDOWMENT 42-43, 47 (2024), https://carnegieendowment.org/research/2024/02/koreas-path-to-digital-leadership-how-seoul-can-lead-on-standards-and-standardization?lang=en.

risk-based approach to cybersecurity and that South Korea engage in public-private partnerships to overcome problem areas.[40]

China's regulatory framework includes the Cybersecurity Law (CSL), Personal Information Protection Law (PIPL) and the Data Security Law (DSL). The DSL of the People's Republic of China went into effect in 2021. The DSL defines the basic concepts of data security such as what is important data, data handlers, and data processing. It also establishes a comprehensive data security protection system that includes three key mechanisms for protecting important data, restricting the cross-border transfer of important data, and data security reviews. Data handlers must obtain approval from authorities before transferring important data overseas. Data handlers are also required to conduct data security reviews when constructing large data centers or when providing data processing services to foreign organizations. Companies that operate in China, or that collect or process Chinese citizens' data, need to comply with the DSL.[41]

The GDPR only applies to organizations located in the EU or that target EU residents with their services. In contrast, the PIPL applies to the processing of personal information by all organizations regardless of their location. Also, regarding the level of consent required for the processing of personal information, the GDPR allows for the processing of personal information without consent in certain circumstances such as when the processing is necessary for the performance of a contract or for legal compliance. Yet, the PIPL requires that individuals provide explicit consent for the processing of their personal information, unless one of the law's exceptions applies. The PIPL also imposes stricter requirements on the transfer of personal information outside of China. A security assessment by the Cyberspace Administration of China (CAC) is required for such transfers. This is not required in the GDPR. Intellectual property attorney, Daniel Albrecht, of the Starke IP Company in Beijing, notes that since the PIPL is new, it is not yet clear how it will be interpreted and enforced by the CAC.[42]

Cybersecurity incident reporting laws are becoming increasingly common in the Asia Pacific region. Seng discusses the potential issues of cybersecurity incident reporting laws in four key Asia Pacific jurisdictions: India, China, South Korea, and Singapore. This researcher explains the rationale for cybersecurity incident reporting laws designed to: (1)

---

40. *See generally* Park, Chae & Lee, *supra* note 39; Feigenbaum & Nelson, *supra* note 39 at 44, 46, 49; Natasha Wood, *S. Kor.'s 2024 Cyber Strategy: A Primer*, CTR. FOR STRATEGIC & INT'L STUD. (Aug. 2, 2024), https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer.

41. Jihong Chen & Jiabin Sun, *Understanding the Chinese Data Security Law*, 2.2 INT'L CYBERSECURITY L. REV. 209, 210, 213–14, 217 (2021).

42. Daniel Albrecht, *Chinese First Personal Information Protection Law in Contrast to the European GDPR*, 23(1) COMPUT. L. REV. INT'L 1, 1-5 (2022).

improve organization's cybersecurity posture by encouraging them to identify and mitigate security risks; (2) facilitate the government's response to cyberattacks; and (3) protect individual's privacy and security. The laws in the four study areas vary in scope, requirements, and enforcement mechanisms. India requires notification of cybersecurity events to the government, while China's law only applies to critical infrastructure operators. Seng notes three issues related to cybersecurity incident reporting: (1) there is risk of over-reporting, (2) legal compliance may be burdensome on organizations, and (3) some laws lack clarity.[43]

## III. DATA PROTECTIONS IN THE USA

### *A. California Consumer Privacy Act*

In 2002, California became the first U.S. state to pass a data breach notification law. In 2018 California passed the California Consumer Privacy Act (CCPA) to further protect its citizens. The law is the first of its kind in the U.S. and has become the de facto national standard as federal lawmakers have yet to create similar data privacy laws. The CCPA intends to give consumers greater control over their personal information including transparency into what companies collect. The law also gives consumers control over what companies share. However, the implementation cost, especially to small businesses, might lead some businesses to accept the penalty of non-compliance or stop providing services.[44]

The CCPA as written does not adequately fulfill the need of both consumer data privacy and real consumer protection. Byun focuses on the "complex consumer" – someone who holds the role of personal consumer and business-owner/business-employee. Byun suggests two main amendments to the law: restrict the scope of applicability to exclude small businesses; and exclude purchase history and inferences drawn from the definition of personal information. Byun believes this will result in actual consumer protection, while maintaining the data privacy rights provided to the consumer by the CCPA.[45]

The CCPA definition of personal information is broader than the definition used in most U.S. privacy laws. For example, the CCPA definition of personal information includes information that identifies a consumer to a household as well as *relates to* or *describes* a consumer or

---

43. Nicholas Seng, *Cybersecurity Incident Reporting Laws In The Asia Pacific*, 4(3) INT'L CYBERSECURITY L. REV. 325,329–32 (2023).

44. Yunge Li, *The California Consumer Privacy Act of 2018: Toughest US Data Privacy Law With Teeth?*, 32(1) LOY. CONSUMER L. REV. 177, 178, 192 (2019).

45. Diane Y. Byun, *Privacy or Protection: The Catch-22 of the CCPA*. 32 LOY. CONSUMER L. REV. 246 (2020).

household. Snow pointed out that under the CCPA the requirement to opt-out of sale of your personal information places an unduly heavy burden on the consumer as the consumer would have to identify and contact each company that might have their personal information. Professor Kaminski discusses three challenges the First Amendment could present for the CCPA: (1) much of the data classified as personal information is publicly available, (2) a question of whether data is speech, and (3) the trend toward decreasing regulations.[46]

Sherman Atlas legal counsel, Joanna Kessler, examined the differences between the EU's GDPR and the CCPA. Kessler argues that though the CCPA was imperfectly drafted, it is a move in the right direction. Kessler identified that the CCPA has "several ambiguous and potentially problematic provisions," specifically mentioning First Amendment and Dormant Commerce Clause challenges. The research concludes that the U.S. should adopt a federal standard for data privacy and the passage of the GDPR and the CCPA may make it easier to pass such a law as companies that have previously been opposed to a federal law now support a unified standard instead of having to comply with multiple and potential conflicting standards.[47]

Another argument is that the California Consumer Protection Act (CCPA) should reduce and preferably eliminate the list of exempted organizations, which includes many small and medium-sized businesses, non-profit organizations, universities, government entities, and health institutions. One belief is that exempting these organizations harms the consumer as exempted organizations have no responsibility to inform their patrons of a data breach. Third-party service providers (that many of these exempted organizations already use) are subject to CCPA and provide out-of-the-box CCPA compliance tools; additionally eliminating exceptions would reduce confusion about to whom CCPA applies. Consumer privacy may be further reduced by the California Privacy Rights Act (CPRA) amendment to the CCPA which doubles the number of patrons a business must serve to be included.[48]

The International Association of Privacy Professionals (IAPP) tracks proposed and enacted privacy legislation across the U.S.[49] As of July 22, 2024, nineteen states have passed privacy legislation.[50] Of those

---

46. Margot Kaminski et. al., *Symposium: The California Consumer Privacy Act*, 54(1) L.A. REV. 157, 162, 173–75 (2020).

47. Joanna Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource"*, 93 S. CAL. L. REV. 99, 102 (2019).

48. Brennan Gamwell, *California Consumer Protection Act (CCPA): Narrowing CCPA Exemptions Will Ensure Greater Privacy Protections,* GOLDEN GATE UNIV. L. REV. BLOG (Jan. 18, 2022) https://digitalcommons.law.ggu.edu/ggu_law_review_blog/101/.

49. *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PRO. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last updated 2024).

50. *US State Privacy Legislation Tracker*, INT'L ASS'N PRIV. PRO. (July 22, 2024), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

nineteen, only seven were effective as of July 2024. An additional four states have active bills.[51]

### *B. Efforts in US Federal Legislation*

Efforts for a broad U.S. federal set of regulations have been ongoing. This effort started in 2003 when Senator Dianne Feinstein proposed the first federal data breach notification law, Senate Bill S. 1350 entitled the Notification of Risk to Personal Data Act.[52] This bill was read twice and referred to the Senate's Committee on the Judiciary. In November 2003, hearings were held by the Committee on Judiciary's Subcommittee on Terrorism, Technology and Homeland Security, where no further action took place. During committee hearings the Feinstein bill was witnessed by: Evan Henricks, Editor/Publisher, Privacy Times, Cabin John, Maryland; Mark MacCarthy, Senior Vice President for Public Policy, Visa U.S.A., Inc., Washington, D.C.; and David McIntyre, President and Chief Executive Office, TriWest, Healthcare Alliance, Phoenix, Arizona.[53] Evan Henricks stated in his remarks, "we don't want a consumer protection law to be turned into something that deprives people of hard-fought privacy rights."[54] Another concern raised during the hearing was that many databases are outside the field of business, for example, government databases.[55] The committee also raised a concern about the cost to businesses to provide notifications.[56] These and other concerns, such as states' rights,[57] may have prevented this bill from being enacted.

A second and stronger Feinstein bill, still named the Notification of Risk to Personal Data Act, was introduced in April 2005.[58] The bill proposed allowing individuals to place a seven-year fraud alert on their credit reports.[59] This bill was also not enacted.

Many subsequent bills introduced in the U.S. Congress have had similar results. Legislation proposed in 2015 included the Data Breach

---

51. *Id.*

52. S. 1350, 108th Cong. (2003).

53. *Database Security: Finding Out When Your Information Has Been Compromised: Hearing Before the S. Comm. on the Judiciary's Subcommittee on Terrorism, Technology and Homeland Security*, 108th Cong., 1st Sess. 1-56, at 3, 6-7 (2003).

54. *Id.* at 7.

55. *Id.* at 10.

56. *Id.* at 11.

57. *Id.* at 9 (Hendricks stating "I don't think you really need to out and out preempt state laws because if, first of all, if you do this law, then States will move on and they won't need to enact laws in the States. They will see that the Congress is taking care of it…").

58. Sabrina I. Pacifici, *Sen. Feinstein Introduces Notification of Risk to Personal Data Act*, BESPACIFIC (Apr. 13, 2005), https://bespacific.com/sen-feinstein-introduces-notification-of-risk-to-personal-data-act/.

59. *Id.*

Notification and Punishing Cyber Criminals Act, S. 1027,[60] Federal Exchange Data Breach Notification Act, H.R. 555,[61] and the Personal Data Notification and Protection Act, H.R. 1704.[62] The Data Breach Notification and Punishing Cyber Criminals Act required limited commercial entities to protect unencrypted data, notify individuals upon a data breach and risk of identity theft, financial harm, or unlawful conduct. In addition, these entities would be required to contact the Department of Homeland Security (DHS) if the personal information compromised exceeded 1,000 individuals, a data system with greater than 250,000 accounts, federal databases, or personal information involving national security or law enforcement. The Federal Exchange Data Breach Notification Act required the health insurance exchange to notify their customers of a breach within 60 days of its occurrence, and the proposed Personal Data Notification and Protection Act of 2015 required businesses storing over 10,000 personal records to notify their customers within 30 days of a security breach discovery.

In 2017, The Cyber Breach Notification Act, H.R. 3975,[63] and the Personal Data Notification and Protection Act, H.R. 3806,[64] were introduced. The Cyber Breach Notification Act required entities that use personally identifiable information of their customers provide specified notification if a data breach has occurred. The Personal Data Notification and Protection Act is similar in nature, where businesses must notify federal agencies, credit reporting agencies, and media. Also in 2017, following disclosure of the Uber data breach, three senators introduced the Data Security and Breach Notification Act, S. 2179.[65] This proposed legislation was introduced in the Senate on November 30, 2017 and referred to the Senate's Commerce, Science and Transportation Committee.[66] No further action was taken.

In September 2018, the Consumer Information Notification Requirement Act, H.R. 6743, was introduced requiring a national standard for financial institution data security and breach notification. No additional action occurred after the bill was placed on the House's calendar.[67] H.R. 3806, that proposed a national notification standard, called for nationwide notifications within 30 days of the discovery of a security

60. *See* Data Breach Notification and Punishing Cyber Criminals Act of 2015, S.1027, 114th Cong. (2015).

61. *See* Federal Exchange Data Breach Notification Act of 2015, H.R. 555, 114th Cong. (2015).

62. *See* Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015).

63. Cyber Breach Notification Act of 2017, H.R.3975 115th Cong. (2017).

64. Personal Data Notification and Protection Act of 2017 H.R. 3806, 115th Cong. (2017).

65. Chris Brook, *Following Uber Breach Senators Introduce Data Breach Notification Act* (2020), FORTRA (Dec. 6, 2017), https://digitalguardian.com/blog/following-uber-breach-senators-introduce-data-breach-notification-act.

66. Data Security and Breach Notification Act of 2017, S. 2179, 115th Cong. (2017).

67. Consumer Information Notification Requirement Act, H.R. 6743, 115th Cong. (2017).

breach.[68] The bill proposed that the Federal Trade Commission (FTC) have one year after the law is enacted to establish and implement the required policies and procedures in regulations to protect personal information.

On May 7, 2019, the Data Breach Prevention and Compensation Act of 2019 was introduced in both the Senate, S.1336,[69] and House, HR. 2545.[70] The bill would require credit reporting agencies to notify affected consumers of a breach. No action was taken after the bills were referred to committee.[71]

The 2022 version of The Federal Information Security Management Act, while remaining unchanged since 2014,[72] advances its framework by improving upon clarification of cybersecurity roles, expanding risk posture, providing more effective reporting, improving cyber asset management with situational awareness, and streamlining intra-agency communications. Senate Bill 2251, Federal Information Security Modernization Act of 2023, would require federal agencies to report all cybersecurity incidents.[73]

Understanding the need for clear data breach notification guidelines, multiple federal agencies have implemented their own sector specific standards regarding protection of privacy.

In 2023, the FCC released a Notice of Proposed Rulemaking (NPRM), that will strengthen the existing Commission's regulatory framework for data breaches. This will affect the Telecommunications Relay Services (TRS), where if consumer proprietary network information (CPNI) is compromised resulting in a data breach, the new procedures will be followed.[74] In this NPRM, the following areas are identified for improvement: reducing unintended exposure of consumer information, easing stringent TRS notification requirements to the FCC, ensuring notification to both the Secret Service and FBI agencies, and eliminating delayed breach notification to the consumer. In addition, the FCC adopts harm-based triggers of notification, minimum customer content requirement for notifications, and addresses the degree of what is considered sensitive personal information of the consumer.

Hardening the Health System in 2023, the FTC is proposing a Health Breach Notification Rule (HNBR), which requires a company with a data breach to take the following actions: (1) notify the

---

68. H.R. 3806.

69. Data Breach Prevention and Compensation Act of 2019, S. 1336, 116th Cong. (2019).

70. Data Breach Prevention and Compensation Act of 2019, H.R.2545, 116th Cong. (2019).

71. Chlotia Garrison & Clovia Hamilton, *A Comparative Analysis of the EU GDPR to the US's Breach Notifications*, 28(1) INFO. AND COMM'NS TECH L.J. 99, 99-114, (2019).

72. *See* Federal Information Security Modernization Act of 2022, H.R. 6497, 117th Cong. (2022).

73. Federal Information Security Modernization Act of 2023, S. 2251, 118th Cong. (2024).

74. FCC Data Breach Reporting Requirements, 47 C.F.R. § 64 (2023).

individuals that were breached, (2) notify the FTC, and (3) contact the media for communication in special cases.[75] The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires specific industries to report data breaches to the Cybersecurity and Infrastructure Security Agency (CISA), involving both cyber incidents and ransomware attacks.[76]

The American Privacy Rights Act of 2024 was introduced to the U.S. House and referred to the House Committee on Energy and Commerce on June 25, 2024. This bipartisan draft legislation creates national data privacy rights and protections for Americans. The Act "[g]ives Americans the [a]bility to [e]nforce [t]heir [d]ata [p]rivacy [r]ights", protect their civil rights, hold companies accountable for strong data security, and "[f]ocuses on the [b]usiness of [d]ata, [n]ot [m]ainstreet [b]usiness."[77] The legislation, if passed, however, would not displace the state laws "that address notification requirements in the event of a data breach."[78]

### *C. Artificial Intelligence advancement promotes urgency for a U.S. federal law*

Given the advancements of Artificial Intelligence (AI) and its potential of a greater and more critical role in our modern technological age, we examine the concerns posed by AI. Misinformation, disinformation, privacy, data breaches, and deep fakes are all interrelated concepts that pose significant corporate and national security threats. Misinformation is false or inaccurate information that is spread unintentionally.[79] Disinformation is false or inaccurate information that is spread intentionally to deceive or mislead. Both misinformation and disinformation can be used to undermine public trust in businesses,

---

75. *FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule*, FED. TRADE COMM'N (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

76. *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia (last visited Feb. 12, 2025).

77. Press Release, Maria Cantrell US Senator for Washington, Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation: The American Privacy Rights Act Gives Americans Fundamental, Enforceable Data Privacy Rights, Puts People in Control of Their Own Data and Eliminates the Patchwork of State Laws, https://www.cantwell.senate.gov/news/press-releases/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation (last visited Aug 13, 2024).

78. American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 20(a)(3)(E) (2024).

79. *See* REBECCA J. BLANKENSHIP, DEEP FAKES, FAKE NEWS, AND MISINFORMATION IN ONLINE TEACHING AND LEARNING TECHNOLOGIES 72 (IGI Glob. 2021).

government, institutions, and the media. They can also be used to sow societal discord and division.[80]

Privacy is the right to control one's personal information. Data breaches, which are unauthorized intrusions into computer systems that contain personal information, can compromise privacy, and pose a risk to a company's cybersecurity and to a country's national security. For example, if a data breach exposes the personal information of military or corporate personnel, it could be used by adversaries to target them for espionage or cyberattacks.

Deep fakes are synthetic media that are created using AI to manipulate or generate images, audio, or video of real people. Deep fakes can be used to create fake news, impersonate public figures, or spread disinformation. They can also be used to damage someone's reputation or to manipulate public opinion.[81]

Advanced AI is transforming the way we work and the way we live our lives. Swift Currie's legal counsel, Marissa Merrill, explored the privacy concerns that arise from the use of voice-activated personal assistants (VAPA) like Amazon's Alexa. These devices listen to users' conversations to personalize their experience. But this raises data privacy concerns because the devices can track users' movements, habits, and interests. Merrill discusses how these devices are beneficial because they save users time and effort. Yet the information could be used to target users with advertising or to discriminate against them. In the U.S., although there is no federal law to regulate the privacy of VAPA voice recordings, the FTC has issued guidelines for companies that collect and use voice data. But there are some state regulations to protect consumer privacy rights. Merrill advocates that consumers need to review device privacy policies, use these devices only when necessary, be careful about the commands given to these devices, use a privacy screen or cover when not using these devices, and delete voice recordings regularly[82]

One argument is despite the widespread support for data privacy laws such as the EU's GDPR, consumers do not actually want more data privacy. This researcher cites several studies that show, when given the opportunity, that consumers rarely read privacy policies or opt out of data collection practices. Wilcox advocates that consumers value the convenience and personalization that comes with data collection more

---

80. Sean Dack, *Deep Fakes, Fake News, and What Comes Next*, UNIV. OF WASH. HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES (Mar. 20, 2019), https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/.

81. *Id.*

82. Marissa Merrill, *An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age*, 71 MERCER L. REV. 637, 637–650, (2019); *see also* Clovia Hamilton et al., *Developing a Measure of Social, Ethical, and Legal Content for Intelligent Cognitive Assistants*, 16(3) J. OF STRATEGIC INNOVATION AND SUSTAINABILITY 1–37 (2021).

than they value their privacy. This researcher notes that the consumers that are very concerned about data privacy are in the minority. Wilcox also argues that the GDPR harmed businesses by increasing the legal compliance burden and by making it more difficult to collect and use data. Wilcox does not favor the U.S. adopting a federal law like the GDPR, and argues that the U.S. should enact simpler and more lenient regulations tailored to the specific needs of different industries. Having a federal data privacy law could help to thwart identity theft and other forms of fraud.[83]

Despite these positives, a fear of losing control still looms. For example, Italy banned ChatGPT because the AI chatbot caused data breaches and violated data protection regulations.[84] Furthermore, the EU and China are developing an artificial intelligence regulation. The EU's regulation includes a "ban on the use of the technology in biometric surveillance and for generative AI systems like ChatGPT to disclose AI-generated content."[85] It will likely take years to put in place the right protections.[86] Contrary to the EU, China has censorship and desires more oversight over artificially intelligent systems that enable democratic discourse.[87]

In March 2023, some high-tech firms began signing a letter advocating the need to slow down and take a six-month pause in the development of artificially intelligent applications. Opponents of the letter, such as Bill Gates, believe that stopping R&D is misguided because AI can be used for good. Gates advocates that the technology private sector and governments can work on solutions to ensure that AI is used for good.[88] Rather, the release of these applications into the general public (where the actual harm can occur) should be regulated. Silicon Valley investor Roger McNamee, an early investor in Facebook and advisor to Mark Zuckerberg, characterizes the release of ChatGPT into the general

---

83. Katherine M. Wilcox, *'Hey Alexa, Do Consumers Really Want More Data Privacy?': An Analysis of the Negative Effects of the General Data Protection Regulation*, 85 BROOKLYN L. REV. 257, 260, 274-77, (2019).

84. Juliana Kim, *ChatGPT Is Temporarily Banned in Italy Amid an Investigation Into Data Collection*, NPR (Mar 31, 2023), https://www.npr.org/2023/03/31/1167491843/chatgpt-italy-ban-openai-data-collection-ai.

85. Foo Yun Chee & Supantha Mukherjee, *Europe Has Taken A Major Step Towards Regulating AI*, WORLD ECON. F. (Jun 19, 2023), https://www.weforum.org/stories/2023/06/eu-artificial-intelligence-ai-rules/.

86. Claudi L. Bockting et al., *Living Guidelines For Generative AI — Why Scientists Must Oversee Its Use*, 622 NATURE 693, 693–696, (26 October 2023).

87. Rebecca Arcesati & Wendy Chang, *China Is Blazing a Trail in Regulating Generative AI – on the CCP's Terms*, THE DIPLOMAT (April 28, 2023) https://thediplomat.com/2023/04/china-is-blazing-a-trail-in-regulating-generative-ai-on-the-ccps-terms/.

88. Robert Hart, *Elon Musk and Tech Leaders Call for AI 'Pause' Over Risks to Humanity*, FORBES (Mar. 24, 2023), https://www.forbes.com/sites/roberthart/2023/03/29/elon-musk-and-tech-leaders-call-for-ai-pause-over-risks-to-humanity.

public as an uncontrolled experiment without regulatory guardrails.[89] ChatGPT's founder OpenAI CEO, Sam Altman, appeared before a U.S. Senate hearing and stated that there is an urgent need and regulation should be accelerated.[90]

Geoffrey Hinton, known as the Godfather of AI, built the neural network that operates like a brain that is used in ChatGPT. In May 2023, Hinton announced that a part of him regrets his life work in AI because although AI is useful, if applications are developed that are more intelligent than humans, those applications gain control. Bill Gates has stated that concerns about AI becoming super intelligent and outpacing or exceeding human capabilities is a legitimate concern but that we are not there yet.[91] However, Hinton advocates that it is important to mitigate the long-term risks.[92] In late May 2023, it was reported that Geoffrey Hinton has stated that society should be worried, and the rapid pace of AI development should be a wakeup call to regulators that legislation is too slow to emerge.[93]

Apple's cofounder Steve Wozniak weighed in on this topic and stated that artificially intelligent applications will make scams more convincing and harder to spot; and malicious intrusions more prevalent.[94] UNC Chapel Hill law professor Ifeoma Ajunwa is concerned about AI privacy issues and states that the U.S. lags behind the EU in regulatory efforts[95] In May 2023, there was a U.S. Congressional hearing on AI to discuss the need for a regulatory framework of AI guardrails. Missouri Republican Senator Josh Hawley stated "we've got to give Americans some basic digital privacy rights, and we've got to stop the tracking and the buying and selling of private information without users' consent. I mean, that's just critical. And now we have AI on top of that."[96]

---

89. Roger McNamee, *There Is Only One Question That Matters with AI*, TIME (Apr. 5, 2023), https://time.com/6268843/ai-risks-democracy-technology/.

90. James Clayton, *AI Regulation Hearing*, BBC NEWS, (May 17, 2023), https://www.bbc.com/news/world-us-canada-65616866.

91. Bobby Allyn, *The Godfather of AI Warns of its Dangers,* NPR (May 27, 2023), https://www.npr.org/2023/05/27/1178575886/-the-godfather-of-ai-warns-of-ai-possibly-outperforming-humans.

92. *Id.*; *see also* Scott Tong, *Warnings About the Power of Artificial Intelligence from the 'Godfather of AI'*, NPR: WBUR (May 26, 2023), https://www.wbur.org/hereandnow/2023/05/26/godfather-ai-warning.

93. Tong, *supra* note 92.

94. Philippa Wain, *Apple Co-founder Says AI may Make Scams Harder to Spot*, BBC (May 8, 2023), https://www.bbc.com/news/technology-65496150.

95. Claudia Grisales, *Congress Wants to Regulate AI, but It Has a Lot of Catching Up to Do*, NPR (May 15, 2023), https://www.npr.org/2023/05/15/1175776384/congress-wants-regulate-ai-artificial-intelligence-lot-of-catching-up-to-do.

96. A. Martinez & Claudia Grisales, *Capitol Hill Hearings to Take a Closer Look at Guardrails for Artificial Intelligence,* NPR (May 16, 2023), https://www.npr.org/2023/05/16/1176371658/capitol-hill-hearings-to-take-a-closer-look-at-guardrails-for-artificial-intelli.

Yet, some U.S. legislators such as Senator Marco Rubio believe that while we cannot put genies back in bottles, it is too early to set regulations. He advocates that Congress needs to better understand what it is dealing with first.[97] In late July 2023, seven high-tech companies signed a voluntary agreement of commitment in cooperation with the U.S. White House on parameters on how to roll out AI applications. There is a need for more transparency, system testing, limited use, disclosure of known risks, leadership to address issues of national security, and mechanisms to hold companies liable. These parameters included committing to using watermarks, privacy protections, means to guard against bias, and to have independent third parties conduct external checks. Their goal is to prevent their products from jeopardizing U.S. security. The U.S. White House stated that an executive action is forthcoming to include federal agency guidance.[98]

The combination of these factors poses a serious threat to cybersecurity. Adversaries can use misinformation, disinformation, privacy violations, data breaches and deep fakes to undermine public trust in companies, governments, and other institutions;[99] sow discord and division within society;[100] target individuals for espionage[101] or cyberattacks;[102] damage reputations;[103]influence people and destabilize democracies;[104] and even influence national elections,[105] executive appointments, and hiring. In addition, adversaries can use these techniques to disrupt critical infrastructure. For example, there is a risk that

---

97. Senator Marco Rubio, *Congress Should Think Before it Regulates AI*, WASH. TIMES (Sep. 25, 2023), https://www.washingtontimes.com/news/2023/sep/25/congress-should-think-before-it-regulates-ai/.

98. Deepa Shivaram, *Biden and Tech Leaders Announce Commitments to Manage Artificial Intelligence*, NPR (July 21, 2023), https://www.npr.org/2023/07/21/1189450171/biden-and-tech-leaders-announce-commitments-to-manage-artificial-intelligence.

99. *See* David V. Gioe, et al., *Pride of Place Reconceptualizing Disinformation as the United States' Greatest National Security Challenge*, 9(3) PRISM 141–157 (2022).

100. *Id*. at 141; *see also* Brian Bennett, *Exclusive: Iran Steps Up Efforts to Sow Discord Inside the U.S.*, TIME (June 9, 2021), https://time.com/6071615/iran-disinformation-united-states/.

101. *See generally* Joe Devanny, et al., *On the Strategic Consequences of Digital Espionage*, 6(3) J. OF CYBER POL'Y 429-450 (2021).

102. *Why Disinformation is a Cybersecurity Threat*, EU DISINFOLAB (May 24, 2021), https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/.

103. Joris van Hoboken & Ronan O Fathaigh, *Regulating Disinformation in Europe Implications for Speech and Privacy*, 6 U.C. IRVINE J. INT'L, TRANSNAT'L & COMP. L. 9, 25 (2021).

104. Brian Bennett, *Exclusive: Iran Steps up Efforts to Sow Discord Inside the U.S.*, TIME (June 9, 2021), https://time.com/6071615/iran-disinformation-united-states/.

105. Caroline Atkinson, et al., *Recommendations to the Biden Administration: On Regulating Disinformation and Other Harmful Content on Social Media,* (Harv. Kennedy School Mossavar-Rahmani Center For Bus. & Govt., Working Paper No. 02, 2021).

an AI application can cause a breach and take over a power grid or supercharge the spread of misinformation creating panic.[106]

These threats are only going to become more severe as technology advances. It is important for businesses, governments, and individuals to take steps to mitigate these risks. Given that the U.S. does not have a national data protection regulation like the EU's GDPR, based on this research, there are multiple ways individuals can mitigate the cybersecurity risks of misinformation, disinformation, privacy, data breaches, and deep fakes.

We should promote media literacy and critical thinking skills because people need to be able to identify and evaluate data and information from a variety of sources. Individuals should consult fact-checking and data protection organizations to identify and debunk false information. Digital users should protect personal information with strong passwords and be careful about the information shared online. Individuals should be aware of the risks of deep fakes and be more skeptical of images, audio and video that seem too good to be true. Likewise, individuals should report suspicious activity to the appropriate authorities.

Businesses and institutions can invest in research and develop new technologies to detect and debunk false information, educate the general public about the dangers of cybersecurity threats, and advocate for stronger laws and regulations to protect personal information. The challenge of addressing data and information protection is complex and multifaceted. However, it is essential that steps be taken to provide better protection and ultimately to protect democracies.

## IV. CHARACTERISTICS OF THE LAST ENACTED US STATE LAWS

Due to the increase in data breaches, state privacy and breach notification legislation has continued to evolve and now exists in all fifty states. Before 2005, only one state had passed a data breach notification law. The last two states did not pass a data breach notification law until 2018.[107] Thus, in the U.S., when a data breach occurs, companies must consider the multiple individual U.S. state laws that apply to their customers.

Alabama and South Dakota were the last two states to pass data breach notification laws.[108] Alabama's law became effective on June 1,

106. Guruaghav Raman, et al., *How Weaponizing Disinformation can Bring Down a City's Power Grid*, PLOS ONE (Aug. 12, 2020), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0236517.

107. Bellamy, *supra* note 14.

108. *Id.*

2018[109] and South Dakota's law became effective on July 1, 2018.[110] The other forty-eight states' data breach notification laws began to appear 15 years prior. Thus, these states had the benefit of 15 years of data breach notification laws to use for guidance. They also had the benefit of the EU's GDPR.

We review six key areas covered by the Alabama and South Dakota data breach notification laws. These include (1) the definition of security breaches; (2) definition of personal information; (3) notice of timeline and exceptions; (4) method of delivery; (5) required notification language; and (6) penalties.

### *A. Definition of Security/Data Breaches*

Alabama's definition of a security breach is the "unauthorized acquisition of data in electronic form containing sensitive personally identifying information."[111] South Dakota's definition is the "unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder."[112] In comparison, the EU's GDPR defines a personal data breach as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[113]

### *B. Definition of Personal Information*

The definition of personal information includes the elements each state identifies as the information that would enable a person to commit identity theft. South Dakota uses two terms: 'personal information' and 'protected information'. These two terms are used together throughout the South Dakota data breach notification law. The definition of protected information includes two elements. The first is username and email address with any required information needed to access an online account. The second facet is financial account numbers.

However, these are also listed in the definition of personal information.[114] South Dakota defines personal information as:

> [A] person's first name or first initial and last name, in combination with any one or more of the following data elements:

---

109. S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018).
110. S.D. CODIFIED LAWS §§ 22-40-20, 22-40-46 (2018).
111. ALA. CODE § 8-38-2 (2019).
112. S.D. CODIFIED LAWS § 22-40-19(1) (2018).
113. General Data Protection Regulation, 2016/679, art. 4, 2018 O.J. (L 119) 12.
114. S.D. CODIFIED LAWS § 22-40-19(4)(2018).

(a) Social security number;
(b) Driver license number or other unique identification number created or collected by a government body;
(c) Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account;
(d) Health information as defined in 45 CFR 160.103; or
(e) An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes.[115]

Alabama uses the term 'sensitive personally identifying information' defined as:

> [A]n Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident:
>
> 1) A non-truncated Social Security number or tax identification number.
> 2) A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.
> 3) A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.
> 4) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
> 5) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
> 6) A username or email address, in combination with a password or security question and answer that would

115. *Id.*

> permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.[116]

Both Alabama's and South Dakota's statutes exclude information that is encrypted unless the key has also been compromised.

Alabama's statute includes the requirement for information holders to implement and maintain measures to protect personal information. A specific list of considerations is provided including designating an individual or individuals to coordinate the security measures, risk identification and mitigation procedures, and continued evaluation and update of internal security measures.[117]

### *C. Notice Deadlines and Exceptions*

Alabama's statute states that the covered entity shall provide notice within forty-five days.[118] In addition, federal and state law enforcement can delay the notification with a written request if the notification would interfere with a criminal investigation or with national security.[119] A third party that experiences a breach must notify the information holder within ten days of the discovery of a data breach. [120]

In comparison, South Dakota requires that residents must be notified not later than sixty days following discovery or notification of a breach.[121] The notification may be delayed by law enforcement if it will hinder a criminal investigation.[122] If delayed by law enforcement, the notification shall be made not later than thirty days after an all clear from law enforcement.[123]

### *D. Methods of Delivering Notices of Data Breaches*

Alabama's law provides that notification must be written, sent to a mailing address or emailed to the address contained in the data holder's records.[124] Alternative broadcast methods are allowed if the cost would exceed $500,000 (USD), the number of individuals to be notified exceeds 100,000, or contact information is not sufficient.[125] In comparison,

---

116. ALA. CODE § 8-38-2(6) (1975).
117. *Id.* § 8-38-3.
118. *Id.* § 8-38-5(b).
119. *Id.* § 8-38-5(c).
120. *Id.*
121. S.D. CODIFIED LAWS § 22-40-20 (2018).
122. *Id.* § 22-40-21 (2018).
123. *Id.*
124. ALA. CODE § 8-38-5(d) (1975).
125. *Id. §* 8-38-5(e).

South Dakota's law states that notification may be written or electronic.[126] Email is identified only as an alternative notification method.[127] The allowance for alternate methods is similar to those for Alabama except that the cost must exceed $250,000 (USD) versus Alabama's $500,000; and the number of individuals must exceed 500,000 in contrast to Alabama's 100,000.[128]

### *E. Required Minimum Content of the Notification*

In Alabama, covered entities must include the following information in their notifications to residents: the date of the breach; a description of the personal information acquired; a description of the actions taken to restore the security and confidentiality of the personal information; a description of identity theft protection steps; and contact information of the covered entity usable for inquiring about the breach.[129] In contrast, South Dakota does not provide any requirements for the contents of the notification to individuals.[130]

### *F. Penalties*

In Alabama, a violation is an unlawful trade practice.[131] Violators are "liable for a civil penalty of not more than… $5,000 per day for each consecutive day" of noncompliance.[132] Civil penalties may not be greater than $500,000 per breach.[133] In South Dakota, the attorney general may prosecute each failure to disclose as a deceptive act or practice and may bring an action to recover on behalf of the state a civil penalty of not more than $10,000 per day per violation.[134]

As of March 2018, all fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach notification laws.[135] Next, the methodology is presented.

---

126. S.D. CODIFIED LAWS § 22-40-22 (2018).

127. *Id.*

128. *Id.*

129. ALA. CODE § 8-38-5(d)(1-5) (1975).

130. *See* S.D. CODIFIED LAWS § 22-40-23 (2018) (explaining that there is compliance if the "information holder maintains its own notification procedure as part of an information security policy" and notifies each person in accordance with its policies).

131. ALA. CODE § 8-38-9(a) (1975).

132. *Id* § 8-38-9(b)(1).

133. *Id.* § 8-38-9(a)(2), (b)(1) (2018).

134. S.D. CODIFIED LAWS § 22-40-25 (2018).

135. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGIS. (Jan. 17, 2022), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

## V. METHODOLOGY

The data breach notification laws of the fifty states have both similarities and differences.

Many state laws share a common language but also omit some currently common aspects. The laws provide definitions of terms such as breach and personal information. They specify when a notification is required, how individuals may be notified (with exceptions for exceeding a specified cost or number of persons), when notification is not required, substitute methods of notification, and when it may be delayed ("legitimate needs of law enforcement" or to determine the scope of the breach and to restore the reasonable integrity of the system). Some identify a specific timeframe for the notification versus the commonly used phrase "without unreasonable delay." Regarding violations, some laws impose minimum or maximum dollar amounts while others impose graduated penalties, with larger penalties for willful violators. Some laws just have general language that allows for prosecutions—the right to bring an action for civil penalties, action in law or equity, and unfair or deceptive trade practice.

Most states do not include paper in their definition of data / security breach though many security breaches are of unauthorized access or exposure of non-computerized data. Between 2007 and 2017 there was an annual average of 94.3 paper data breaches or about 16% of the total number of breaches.[136] Figure 1 shows the number of paper data breaches by year.

136. *Identity Theft Resource Center Data Breach Reports*, IDENTITY THEFT RES. CTR. (2007–2017), https://www.idtheftcenter.org.

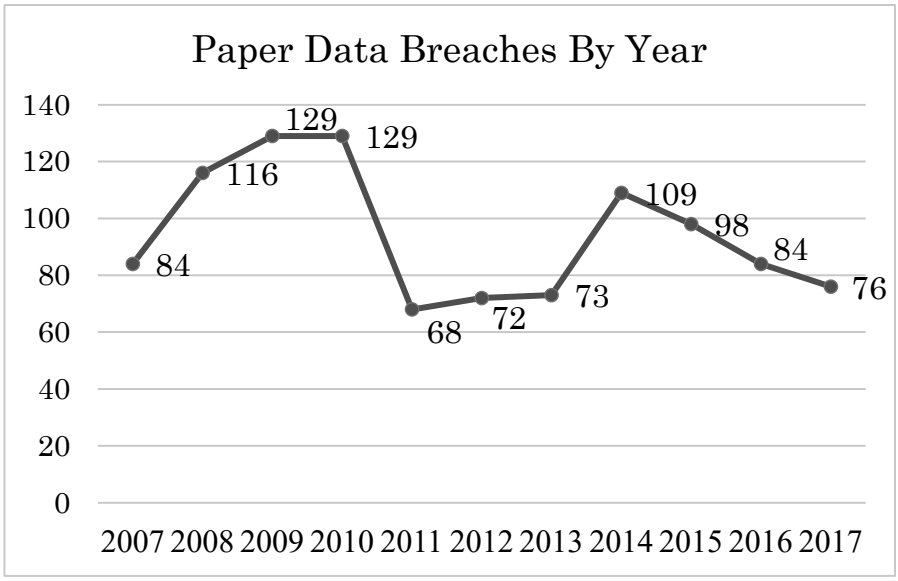



**Figure 1**

Source: Compiled from Identity Theft Resource Center Annual Reports[137]

There are four broad categories of data breach notification laws: definitions and scope, safe harbors and exemptions, notification flow, and penalties.[138] Enacting data breach notification laws can reduce the rate of identity theft.[139] Adopting data breach notification laws can also impact future stock price crash risk.[140]

This article reviews specific changes in the laws of the fifty states from 2003 - 2018. Three research questions guided this survey: (1) Have the laws changed from their original passage to the current content? (2) Is there a relationship between the contents of the law and when the law was passed? (3) Did the party in control influence the passage of a data breach notification law? Thus, we hypothesize that: (1) The contents of the laws have changed from their original content, (2) There is a relationship between the contents of the law and when the original law was passed, and (3) A specific party in control would dominate during the times data breach notification laws were enacted.

---

137. *Id.*

138. Fabio Bisogni et al.,*Estimating the Size of the Iceberg from its Tip: An Investigation Into Unreported Data Breach Notifications*, WORKSHOP ON THE ECON. OF INFO. SEC. (2017).

139. Fabio Bisogni & Hadi Asghari, *More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws*, 10 J. OF INFO. POL'Y 45(2020).

140. Hung Cao, et al., *Data Breach Disclosures and Stock Price Crash Risk: Evidence from Data Breach Notification Laws*, 93 INT'L REV. OF FIN. ANALYSIS 2 (2024).

The legislative sites of each of the fifty states were reviewed to locate the original notification laws. This search was facilitated using the Security Breach Notification Chart maintained by the law firm Perkins Coie.[141] The information maintained by the National Conference of State Legislatures (NCSL) on Security Breach Notification Laws also aided in locating original and current laws.[142] The original and current notification laws from 2003-2018 were analyzed to determine the following content aspects: personal information (PI) defined with medical/health, PI defined with biometric data, specific timeline for notification, specific information that should be included with the notification, revision of PI definition, and revision of breach definition. We analyzed the content of the laws to determine if they have changed from their original content.

To determine if there is a relationship between the contents of the law and when the law was passed, we examined the statistical relationship between the initial scope of states' data breach notification laws and the year of their enactment. In doing so, we ask whether there exist any long-run trends in the regulatory expansion of biometrics, restricted reporting deadline and health/medical information. We discuss the combination of the three as regulatory strictness. We employ a regression analysis approach to estimate the statistical relationship between regulatory strictness of data breach notification laws and the base year of law adoption.

In statistics, regression first appears with Francis Galton, a British polymath, who studied the relationship between the height of parents and their children.[143] Since then, regression analysis has become part of the standard toolkit in natural and social sciences, and has been used to answer sundry research questions in fields as diverse as economics,[144]

---

141. *See* Amelia M. Gerlicher & Todd M. Hinnen, *Security Breach Notification Chart*, PERKINS COIE (2018), https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

142. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATORS (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

143. *See* Francis Galton, *Family Likeness in Stature*, PROC. OF THE ROYAL SOC'Y OF LONDON (1886).

144. *See generally* Casey B. Mulligan & Andrei Shleifer, *Conscription as Regulation*, 7(1) AMERICAN L. AND ECON. REV. 85 (2005).

sociology,[145] biology,[146] linguistics,[147] medicine,[148] and law,[149] among other disciplines. The next section presents the results, starting with an analysis of the contents of the laws.

## VI. RESULTS

### *A. Content Analysis*

#### 1. Legislation Timeline

California was the first state to pass a law that required notification following the discovery of a breach of personal information.[150] The law was signed by the governor on September 26, 2002, and became effective July 1, 2003. The law was prompted and supported by a 108% increase in identity theft cases; the Los Angeles County Sheriff's Department received 1,932 identify theft cases in 2000.[151] Figure 2 shows that a majority of the laws were signed in 2005 and 2006. However, it took until 2018 for all states to enact a data breach notification law.

145. *See generally* Suzanne M. Bianchi, et al., *Is Anyone Doing the Housework? Trends in the Gender Division of Household Labor*, 79(1) SOC. FORCES 191 (2000).

146. *See generally* HARVEY MOTULSKY & ARTHUR CHRISTOPOULOS, FITTING MODELS TO BIOLOGICAL DATA USING LINEAR AND NONLINEAR REGRESSION: A PRACTICAL GUIDE TO CURVE FITTING (Oxford Univ. Press, 2004).

147. *See generally* Pedro Aceves & James Evans, *Human Languages with Greater Information Density Have Higher Communication Speed but Lower Conversation Breadth*, 8 NATURE HUM. BEHAV. 644 (2024).

148. *See generally* Steven C. Bagley, et al., *Logistic Regression in the Medical Literature: Standards for Use and Reporting, with Particular Attention to One Medical Domain,* 54(10) J. OF CLINICAL EPIDEMIOLOGY 979, 979–980 (2001).

149. *See generally* Franklin M. Fisher, *Multiple Regression in Legal Proceedings*, 80(4) COLUM. L. REV. 702 (1980).

150. *The Past, Present, and Future of Security Breach Notification Laws*, MCCUNE LAW GROUP (Apr. 4, 2016), https://www.mccunewright.com/blog/2016/april/the-past-present-and-future-of-security-breach-n/.

151. 2002 Cal. Legis. Serv., Ch. 1054–A.B. 700, at 2 (West).

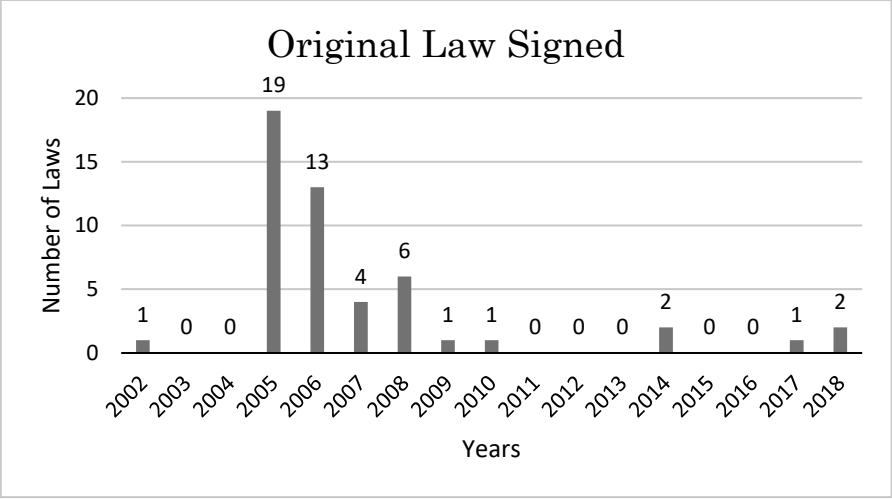



**Figure 2**[152]

2. Legislation Changes

To determine if the contents of the laws have changed from their original passage we determined if the law had been amended. This review was aided by the Security Breach Notification Chart maintained by the law firm Perkins Coie.[153] In addition, we compared the content of each current law versus the law as originally passed. Between 2003 and 2018, thirty-five states amended their breach notification laws. Thirteen states have amended their laws at least twice and one state, California, had amended the law four times; California is also the state with the oldest law. No laws passed after 2008 had been amended through 2018. The next sections analyze specific content changes.

3. Definition of Personal Information

a. Biometric Data

Biometric data is defined by Colorado as "[d]ata generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account."[154] Oregon used the following in their definition of personal information: "[d]ata from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction."[155]

152. *Security Breach Notification Chart*, PERKINS COIE (2018), https://perkinscoie.com/insights/publication/security-breach-notification-chart.

153. *Id.*

154. H.B. 18–1128 at 3 (Colo. 2018).

155. Or. S. B. 1551–ORS 646A.602, 79th Assemb., at 3 (2018).

Through 2018, thirteen of the fifty states include biometric data in their definition of personal information for purposes of defining a security breach.[156] Two states, Kentucky and Washington, have separate statutes for state agencies that include biometrics in combination with other data in the definition of PI.[157] Only five states included biometric data in their original definition of personal information for breach purposes.[158] Texas includes biometric data in its definition of *Personal Information* but not in the term *Sensitive Personal Information* which is used in its breach definition.[159] Of the last three states to pass laws, Alabama and South Dakota in 2018 and New Mexico in 2017, two of the three, New Mexico and South Dakota, include biometric data.[160] The states that included an individual's unique biometric data in their initial definition of Personal Information were signed in 2006, 2008, 2017, 2018.[161] Interestingly, in 2006, Wisconsin not only included medical information but also DNA in its PI definition.[162]

156. The thirteen states are Arizona, Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, Oregon, South Dakota and Wyoming. *See* Ariz. Rev. Stat. Ann. § 18-551(11) (2018); COLO. REV. STAT. ANN. § 6-1-716(1) (West 2018); DEL. CODE ANN. tit. 6, § 12B-101 (2018); 815 ILL.COMP. STAT. ANN. 530/5 (WEST 2017); IOWA CODE § 715C.1 (2018); MD. CODE ANN., COM. LAW § 14-3501 (West 2022); NEB. REV. STAT. ANN. § 87-803 (West 2016); N.M.STAT. ANN. § 57-12C-2 (West 2017); OR. REV. STAT. § 646A.600; S.D. CODIFIED LAWS § 22-40-19 (2018); WIS. STAT. ANN. § 134.98 (West 2008); WYO. STAT. ANN. § 40-12-501 (West 2024).

157. KY. REV. STAT. ANN. § 61.931 (West 2015); WASH. REV. CODE ANN. § 42.56.590 (West 2020).

158. The five states are Iowa, Nebraska, New Mexico, South Dakota, and Winsconsin. *See* IOWA CODE ANN. § 715C.1 (2008); NEB. REV. STAT. § 87-803 (2006); N.M. STAT. ANN. § 57-12C-2 (2017); S.D. CODIFIED LAWS § 22-40-19 (2018); WIS. STAT. ANN. § 134.98 (West 2008).

159. TEX. BUS. & COM. CODE ANN. § 521.002 (West 2023).

160. N.M.STAT. ANN. § 57-12C-2 (West 2017); S.D. CODIFIED LAWS § 22-40-19 (2018).

161. WIS. STAT. ANN. § 134.98 (West 2006); IOWA CODE ANN. § 715C.1 (2008); N.M.STAT. ANN. § 57-12C-2 (West 2017); S.D. CODIFIED LAWS § 22-40-19 (2018).

162. WIS. STAT. ANN. § 134.98 (West 2006).

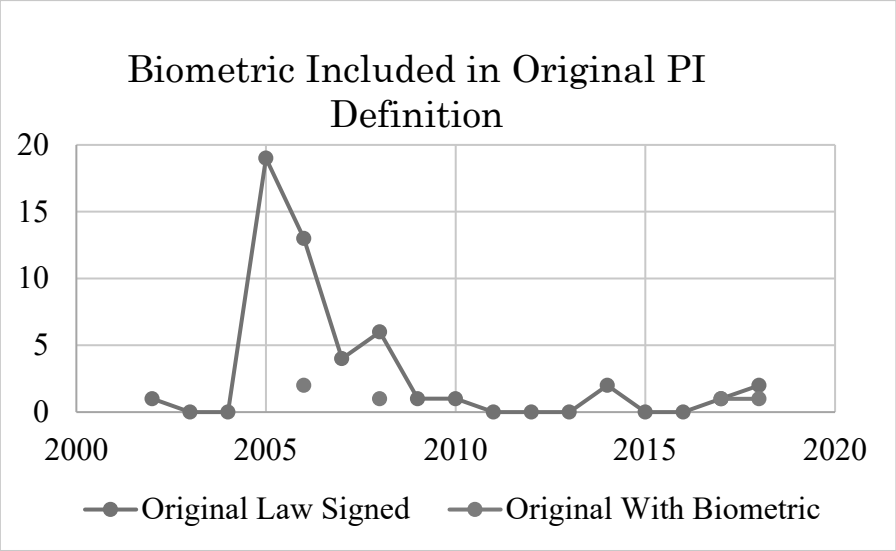



**Figure 3**[163]

Figure 3 shows when the original laws were signed and when the original laws included biometric information in their PI definition. Though no states included biometric information in their definition of PI from 2009 – 2016, a greater percentage of the new laws include biometric data in their definition of personal information. Between 2002 and 2008, forty-three states added data breach notification laws with

163. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171 (West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732, 59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess. (Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

only three of them including biometric data.[164] Between 2009 and 2018, seven additional states passed data breach notification laws with two of these including biometric data.[165]

Figure 4 shows that the early adopters, states with laws added between 2002 and 2008, are also the states that have added biometric information to their definition of PI. None of the seven states that added data breach notification laws from 2009 to 2018 amended their laws to add biometric information to the PI definition. In contrast, eight of the early adopter states added biometric information to their PI definition.

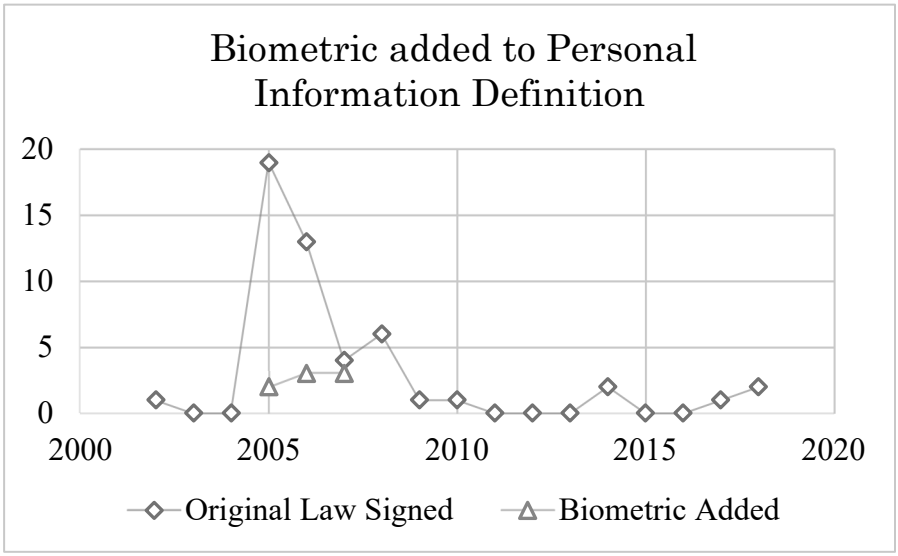



**Figure 4**[166]

164. *Data Breach Notificaton Laws by State*, IT GOVERNANCE USA, https://www.itgovernanceusa.com/data-breach-notification-laws#:~:text=California,-California%20Civil%20Code&text=Enacted%20in%202002%2C%20California's%20data,acquisition%20of%20unencrypted%20personal%20information.

165. *Id.*

166. An Act Improving Data Security and Agency Effectiveness, 2015 Conn. Pub. Acts 15-142 (S.B. 949); Confidential or Privileged Information—Security—Breaches, 2018 Ariz. Legis. Serv. Ch. 177 (H.B. 2154); Georgia Personal Identity Protection Act, 2007 Ga. Laws (S.B. 236); California Bill Analysis, 2016 A.B. 2828 Sen.; 149 Del. Laws H.B. 180 (2017); Florida Information Protection Act of 2014, 2014-189 Fla. Laws (S.B. 1524); Assembly Amendment No. 244 to Assembly Bill No. 179, 2015 Nev. Stat A.B. 179; Ind. Code § 24-4.9 (2017); Minn. Stat. § 325E.61 (2006); Maryland Personal Information Protection Act, 2017 Md. Laws Chapter 518, (H.B. 974); Personal Information Protection Act, 2017 Ill. Laws Pub. Act 100-0412; Computer Data Containing Personal Information – Security Breaches, 2014 Iowa Acts Chapter 1062, S.F. 2259; Credit Report Protection Act, 2018 Neb. Laws LB 757; 2015 Mont. Laws H.B. 74; 2015 N.D. Laws S.B. No. 2214; 2009 Me. Laws H.P. 672, L.D. 970; 2008 Okla. Sess. Laws H.B. No. 2245; 2015 Or. Laws. S.B. 601; 2013 N.Y. Laws § 899-aa; 2009 N.C. Sess. Laws 355 (S.B. 1017); 2006 Ohio Laws S.B. 126; 2013 S.C. Acts H.B. 3248; 2010 Idaho Sess. Laws Ch. 170, p. 346; 2016 Haw. Sess. Laws § 487N; 2014 Kan. Sess. Laws § 50-7a01; Utah Code Ann. § 12-44-101 (West 2017); 2010 Mich. Pub. Acts S.B. 223; 2017 Tenn. Pub. Acts S.B. 547; Va. Code Ann. § 18.2-186.6 (2017); 2015 R.I. Pub. Laws S 0134 Substitute B; 2017 Wash. Sess. Laws H.B. 1717; 2018 La. Acts S.B. 361; 2018 Colo. Sess. Laws H.B. 18-1128; 2015 Mass. Acts

b. Health Data

Health/medical data as used in the definition of personal information includes: (Oregon) "information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer,"[167] and (Texas) "information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual."[168]

Fifteen states include health/medical information in their definition of Personal Information.[169] Five of these states included health/medical information in their original breach notification statute.[170] Figure 5 below shows the number of states that enacted statues with the definition of PI including health/medical information and the year it was enacted. We see from Figure 5 that the only year to have multiple states laws that included health/medical information in the definition of PI was 2018; the last two states to enact data breach notification laws. In addition, over 50%, four of seven, of the states that passed their base or original law from 2009-2018 included health/medical information in the definition of PI. That compares to just 2%, one of forty-three, for 2002-2008. Note that Virginia has a separate breach of medical information notification law, added in 2011.

---

Chapter 93(H); Texas Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521 (West 2013); 2015 Wyo. Sess. Laws S.F. 35 & S.F. 26.

167. OR. REV. STAT. § 646A.602 (2018).

168. TEX. BUS. & COMM. CODE ANN. § 521.002 (West 2023).

169. The fifteen are Alabama, Arizona, California, Colorado, Delaware, Florida, Maryland, Missouri, Montana, North Dakota, Oregon, Rhode Island, South Dakota, Texas, and Wyoming. The respective statutes are: ALA. CODE § 8-38-2 (2018); ARIZ. REV. STAT. ANN. § 18-551(7) (2018); CAL. CIV. CODE § 1798.82 (2023); COLO. REV. STAT. § 6-1-176 (2018); DEL. CODE ANN. tit. 6, § 12B-101(7); FLA. STAT. ANN. § 501.171(g); MD. CODE ANN., COM. LAW § 14-3501 (West 2022); MO. ANN. STAT. § 407.1500(9) (2009); MONT. CODE ANN. § 2-6-1501 (West 2023); OR. REV. STAT. ANN. § 646A.602 (West 2020); tit. no. 11 R.I. GEN. LAWS ANN. § 11-49.3-3 (2023); S.D. CODIFIED LAWS § 22-40-9; TEX. BUS. & COM. CODE ANN. § 521.002(a)(1) (West 2009); WYO. STAT. ANN. § 40-12-501 (West 2024).

170. The five are Alabama, Florida, Missouri, North Dakota, and South Dakota. The respective statutes are: ALA. CODE § 8-38 (2024); FLA. STAT. §§ 501.171 (2024); MO. REV. STAT. § 407.1500 (2009); N.D. CENT. CODE ANN. § 51-30-01 (West 2015); and S.D. CODIFIED LAWS § 22-40-19 (2018).

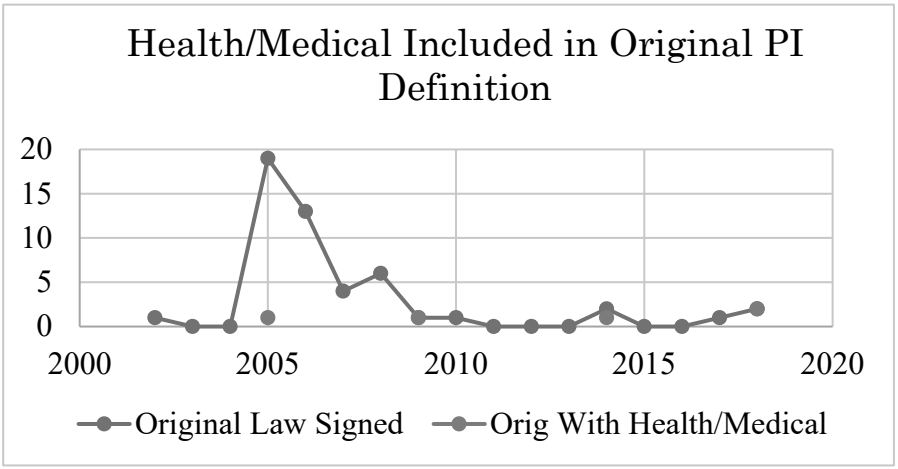
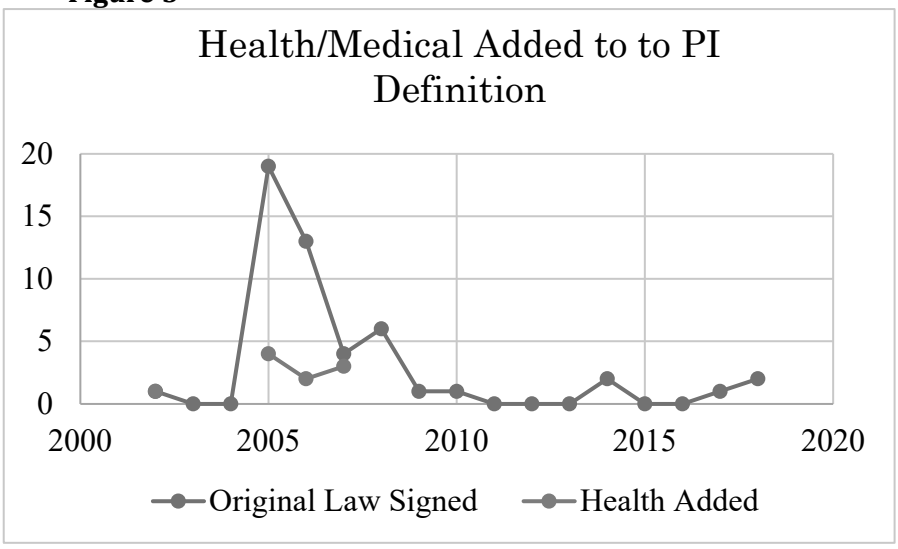



**Figure 5**[171]




171. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171 (West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732, 59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess.

**Figure 6**[172]

Figure 6 shows the number of laws that have been amended to add health/medical information with the year the original laws were passed. We see from Figure 6 that all the amended laws were originally passed between 2002 and 2008. Through 2018, none of the 2009-2018 original laws had been amended to add health/medical. Of the thirteen states that include biometric data, seven also include health/medical information.

4. Restricted Notification Deadline

The timing of the required data breach notification varies. Some states, such as California, specify that the notification should be made "immediately following discovery" or "in the most expedient time possible and without unreasonable delay."[173] States allow a delay if notification would impede a law enforcement investigation, to determine the scope of the breach, and to restore the system's integrity. Other states provide a restricted notification deadline identifying a specific number of days by which the notification must be made.

---

(Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

172. An Act Improving Data Security and Agency Effectiveness, 2015 Conn. Pub. Acts 15-142 (S.B. 949); Confidential or Privileged Information—Security—Breaches, 2018 Ariz. Legis. Serv. Ch. 177 (H.B. 2154); Georgia Personal Identity Protection Act, 2007 Ga. Laws (S.B. 236); California Bill Analysis, 2016 A.B. 2828 Sen.; 149 Del. Laws H.B. 180 (2017); Florida Information Protection Act of 2014, 2014-189 Fla. Laws (S.B. 1524); Assembly Amendment No. 244 to Assembly Bill No. 179, 2015 Nev. Stat A.B. 179; Ind. Code § 24-4.9 (2017); Minn. Stat. § 325E.61 (2006); Maryland Personal Information Protection Act, 2017 Md. Laws Chapter 518, (H.B. 974); Personal Information Protection Act, 2017 Ill. Laws Pub. Act 100-0412; Computer Data Containing Personal Information – Security Breaches, 2014 Iowa Acts Chapter 1062, S.F. 2259; Credit Report Protection Act, 2018 Neb. Laws LB 757; 2015 Mont. Laws H.B. 74; 2015 N.D. Laws S.B. No. 2214; 2009 Me. Laws H.P. 672, L.D. 970; 2008 Okla. Sess. Laws H.B. No. 2245; 2015 Or. Laws. S.B. 601; 2013 N.Y. Laws § 899-aa; 2009 N.C. Sess. Laws 355 (S.B. 1017); 2006 Ohio Laws S.B. 126; 2013 S.C. Acts H.B. 3248; 2010 Idaho Sess. Laws Ch. 170, p. 346; 2016 Haw. Sess. Laws § 487N; 2014 Kan. Sess. Laws § 50-7a01; Utah Code Ann. § 12-44-101 (West 2017); 2010 Mich. Pub. Acts S.B. 223; 2017 Tenn. Pub. Acts S.B. 547; Va. Code Ann. § 18.2-186.6 (2017); 2015 R.I. Pub. Laws S 0134 Substitute B; 2017 Wash. Sess. Laws H.B. 1717; 2018 La. Acts S.B. 361; 2018 Colo. Sess. Laws H.B. 18-1128; 2015 Mass. Acts Chapter 93(H); Texas Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. § 521 (West 2013); 2015 Wyo. Sess. Laws S.F. 35 & S.F. 26.

173. CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2023).

Seventeen states include a specific deadline for notifying affected individuals of a disclosure of their personal information.[174] Five states included the deadline in the original version of the law with another twelve states adding this stipulation through amendments.[175] From Figure 7 below we see that a greater percentage of the new laws include notification deadlines. Just two of forty-three states included a specific notification deadline between 2002 and 2008 while three of seven states that enacted laws from 2009 to 2018 included specific notification deadlines.

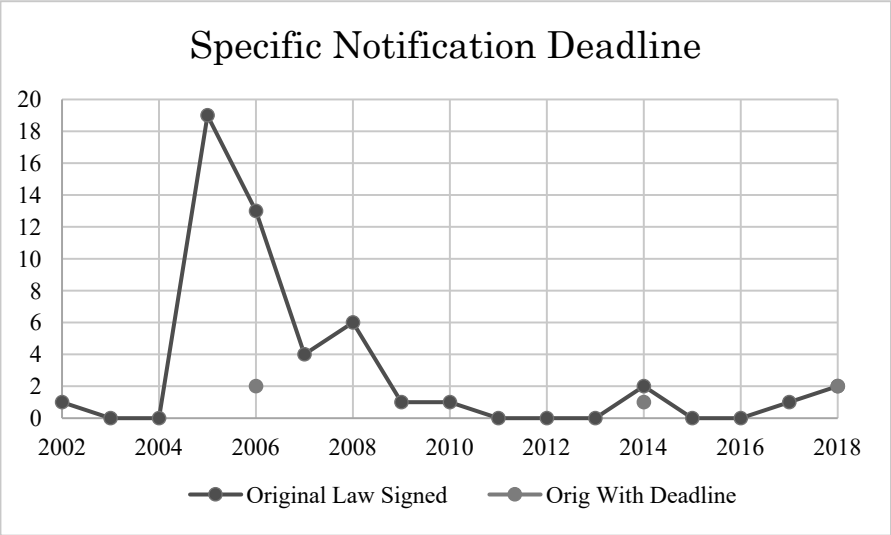



**Figure 7**[176]

174. Colorado and Florida have a 30-day notice requirement; Delaware, Louisiana and South Dakota have the 60-day notice requirement; Connecticut requires a 90-day notice; and the states that require a 45-day notice are: Alabama, Arizona, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont, Washington, and Wisconsin. Maine requires 7-day notice after a law enforcement agency makes a determination (rather than from the discovery date); and California has a 15-day notice requirement for medical information. The respective statutes are: COLO. REV. STAT. ANN.§ 6-1-716 (West 2018) ; DEL. CODE ANN. tit. 6, § 12B-102 (2018); LA. STAT. ANN. § 51:3074 (2018); S.D. CODIFIED LAWS § 22-40-20 (2018); CONN. GEN. STAT. ANN. § 36a-701(b)(1) (West 2015); ALA. CODE § 8-38-6 (2018); ARIZ. REV. STAT. § 18-545 (2016); MD. CODE ANN., COM. LAW §14-3504 (West 2015) ; N.M. STAT. ANN. § 57-12C-6 (West 2017); OHIO REV. CODE. ANN. §1349.19(B)(2)(West 2007); OR. REV. STAT. ANN. §646A.604 (West 2020); 11 R.I. GEN. LAWS ANN. §49.3-4 (West 2015); TENN. CODE ANN. §47-18-2107 (West 2017); VT. STAT. ANN. tit. 9, § 2435 (West 2015) ;WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2015); WIS. STAT. ANN. § 134.98 (West 2018); ME. REV. STAT. ANN. tit. 10, § 1348 (2019); CAL. HEALTH & SAFETY CODE §1280.15(b)(1) (West 2015).

175. The five states are Alabama, Florida, Ohio, South Dakota, Wisconsin. The respective statutes are: ALA. CODE § 8-38-5(b) (2018); FLA. STAT. §§ 501.171, 282.0041, 282.318(2)(i)(West 2024); OHIO REV. CODE ANN., §1349.19(E) (West 2024); S.D. CODIFIED LAWS § 22-40-20 (2024); WIS. STAT. § 134.98(3) (West 2018).

176. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171

Table 2 in the appendix shows the notification deadline by days. We can see that the most common deadline is forty-five days with nearly 65% of states using that deadline. For example, Florida requires thirty days but includes a fifteen-day extension "with cause."[177] Of the seventeen states with a specific numerical deadline, thirty is used twice, sixty thrice, ninety once with the remaining states using forty-five days. For example, the original Connecticut statute, enacted in 2005, states the notification should be made "without unreasonable delay."[178] The law as amended states "without unreasonable delay but not later than sixty days after the discovery of such breach, unless a shorter time is required under federal law."[179] Figure 8 shows that the majority of the states with a specific deadline were signed into law before 2008 and that forty-five days is the most popular number of days before and after 2008. From 2009 to 2018, 50% of the states with specific deadlines selected forty-five. Prior to 2009, 80% selected forty-five days as their notification deadline.

(West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732, 59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess. (Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

177. FLA. STAT. §§ 501.171(3)(a) (West 2024).

178. CONN. GEN. STAT. § 36A-701b(b) (2005).

179. CONN. GEN STAT. ANN. §§ 36a-701b (2025).

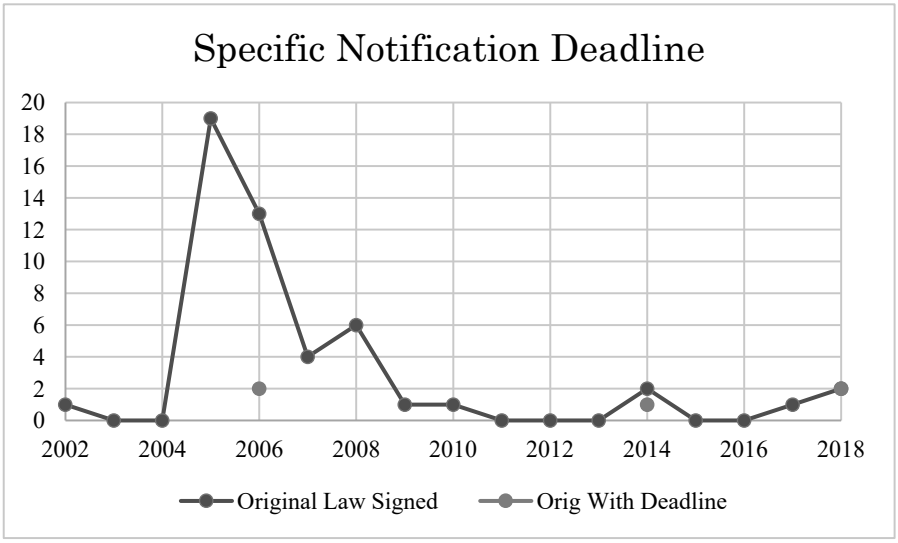



**Figure 8**[180]

5. Additional characteristics

In addition to adding biometric and health/medical information to the definition of PI, various other changes were made to the definition of PI. For example, the expansion of personal numbers (generic or specific). Specific examples are passport, tax ID, government ID number, and tribal ID number. Username and email with access codes that allow

180. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171 (West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732, 59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess. (Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

access to online financial accounts were added. An itemized listing of financial numbers, credit/debit card numbers, demand deposit/savings account numbers, are included in some definitions. Employee ID numbers with security or access codes and encrypted data if the keys are also disclosed are in most definitions of personal information. In general, the personal information definition includes information that is not encrypted.

Twenty-four states provided specifics of what should be included with the notification.[181] The type of information required includes: the approximate date of the breach; a description of the personal information included in the breach; actions taken to restore the security and confidentiality of the information involved in the breach; steps consumers can take to protect themselves from identity theft; toll-free telephone numbers and addresses of the three largest credit reporting agencies; contact information including website for the FTC or other federal agency that assists consumers with identify theft issues and a statement that an individual can obtain information from these sources about steps to avoid ID theft; information the individual can use to contact the covered entity to inquire about the breach; and advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

The above analysis of the laws supports Hypothesis 1 that the laws have changed content from their original passage. Thirty-five laws have been amended with content changes including the definition of personal information and the definition of data breaches.

### *B. Statistical Analysis*

In this section, we examine the second research question: Is there a relationship between the contents of the law and when the law was passed? For this analysis we examine the statistical relationship between the initial scope of states' data breach notification laws and the year of their adoption. In doing so, we ask whether any long-run trends in regulatory expansion vis-à-vis breach definitions, security breach

---

181. The following U.S. states provide guidelines for the content to include in notifications of breaches: (1) ALA. CODE § 8-38-5(d) (2025); (2) ARIZ. REV. STAT. ANN. § 18-552(E) (2025); (3) CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2024); (4) COLO. REV. STAT. ANN. § 6-1-716(2) (West 2025); (5) FLA. STAT. ANN.§§ 501.171(3)(b) (West 2024); (6) HAW. REV. STAT. § 487N-2(d) (West 2024); (7) 815 ILL. COMP. STAT. ANN. 530/10 (West 2024); (8) IOWA CODE ANN. § 715C.2 (West 2024); (9) MD. CODE ANN., COM. LAW §14-3504 (West 2024); (10) MASS. GEN. LAW ANN. ch. 93H, § 1 (2024); (11) MICH. COMP. LAWS ANN. § 445.72 (West 2025); (12) MO. ANN. STAT. § 407.1500(4) (2024); (13) N.H. REV. STAT. ANN. § 359-C:20 (2025); (14) N.M. STAT. ANN. § 57-12C-1 (West 2024); (15) N.Y. GEN. BUS. LAW § 899-AA (McKinney 2025); (16) N.C. GEN. STAT. ANN. § 75-65 (West 2024); (17) OR. REV. STAT. ANN. §646A.604 (West 2024); (18) 11 R.I. GEN. LAWS ANN. §49.3-4 (West 2024); (19) VT. STAT. ANN. tit. 9, § 2435 (West 2025) ; (20) VA. CODE ANN. § 18.2-186.6 (West 2024); (21) WASH. REV. CODE ANN. § 19.255.010 (West 2024); (22) W.VA. CODE ANN. § 46A-2A-102 (West 2025); (23) WIS. STAT. ANN. § 134.98 (2023); (24) WYO. STAT. ANN. § 40-12-502 (West 2025).

notifications to affected individuals, and associated penalties to violators are discernible at the national level. Three such clauses of state base laws for which we found data are considered: (1) Biometrics, (2) Restricted Reporting Deadline, and (3) health/ medical. These terms are as explained individually above. We discuss the combination of the three as regulatory strictness.

Data shows that the enactment of data breach notification laws in the U.S. underwent a spurt across state legislatures during the mid-2000s. In 2005 and 2006 alone, as many as thirty-two states approved data breach notification laws including various elements such as, the definition of security breaches, the meaning of personal information, rules on mandatory customer notification, and penalties to firms or employees for failure to provide said notices.[182] Figure 9 depicts the number of new laws (one per state) enacted in a given year, while Figure 10 shows the cumulative progress in law adoption across all states (i.e., the country). Within six years beginning with 2002, forty-three states had adopted data breach notification laws and as of 2018, such laws are present in all fifty states.[183]

With respect to regulatory strictness, the years 2006, 2014, and 2018 saw the greatest number of the above-named clauses embedded in the states' newly enacted base data breach notification laws (Figure 11).[184] Figure 12 depicts the number of base law clauses across the ten

---

182. *Data Breach Notification Laws by State*, IT GOVERNANCE, https://www.itgovernanceusa.com/data-breach-notification-laws (last updated July 2018).

183. *Id.*

184. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171 (West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732, 59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess. (Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

states that had at least one such clause present.[185] Most of these states are Midwestern (seven), with the remaining three located in the South.

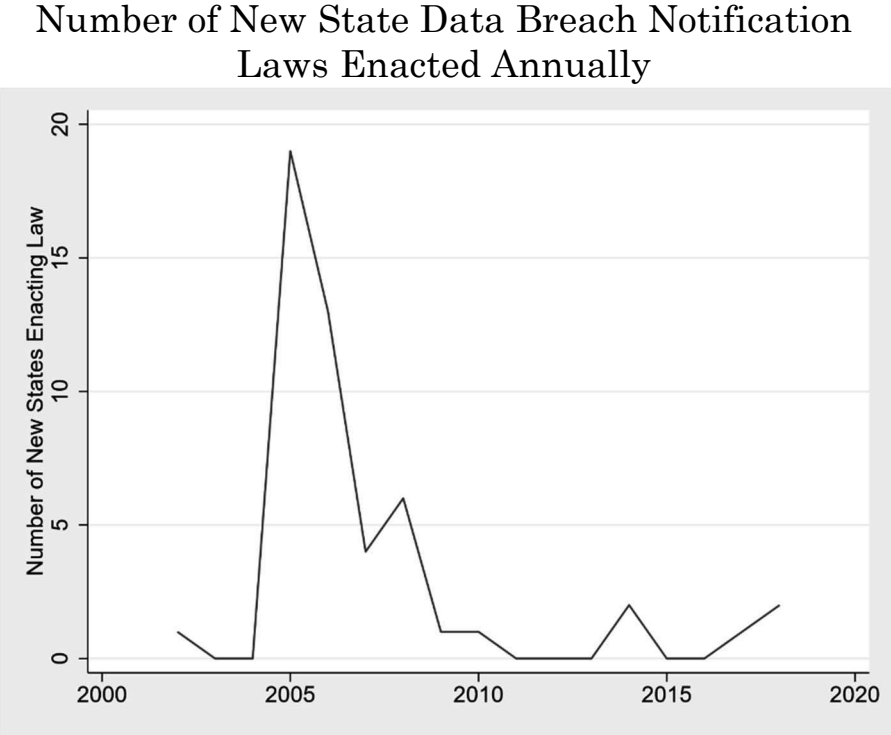



**Figure 9**[186]

185. *Id.*
186. *See id.*

Cumulative Presence of State Data Breach Notification Laws

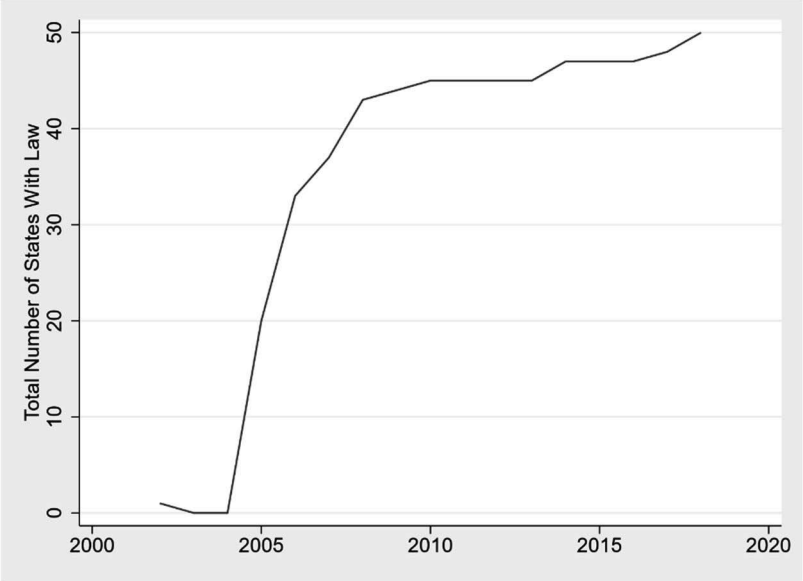



**Figure 10**[187]

Number of Clauses Present in Base Data Breach Laws, All States

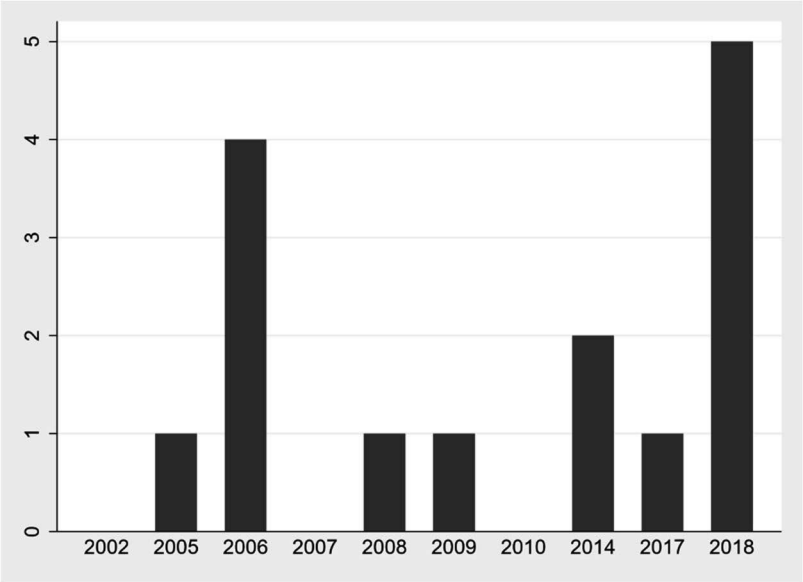



**Figure 11**[188]

187. *Id.*
188. *Id.*




**Figure 12**[189]

To conduct the analysis of regulatory strictness of state base data breach notification laws over time, we employ regression analysis. This statistical procedure allows us to expressly quantify the relation between any two or more variables, and, in our case, answer how the number of clauses in the law is expected to change as the year of adoption changes, enabling us to better understand regulatory trends in this area of law across the country.[190]

The regression analysis stipulates an initial selection of the *response variable*—the one to be explained (regulatory strictness)—and the *explanatory variable*, the one that explains our outcome of interest (the year of law's adoption). The relationship between the response ($Y$) and explanatory ($X$) variables is modelled as a statistical equation, called the regression equation, which standardly includes slope and intercept terms. Generically, $\alpha$ is the intercept, $\beta$ is the slope, and $\varepsilon$ is the "error"

189. *Id.*

190. JAMES H. STOCK & MARK W. WATSON, INTRODUCTION TO ECONOMETRICS 101, 101-23 (Pearson Educ. Ltd., 4th ed. 2018).

term that allows for a degree of uncertainty, or randomness, that is inherent in all statistical relationships. The regression equation itself is a mathematical representation of the line of best fit that illustrates the pattern of the relationship between *X* and *Y*. Regressions may have one or more explanatory variables, in which case they are termed *multiple regressions*.[191]

The next step in regression analysis is to estimate, or compute, the parameters of this equation—the intercept $\alpha$ and the slope $\beta$. It is the estimation step that allows for explicit quantification of the response-explanatory variable relationship. Of particular interest in regression modelling is the correct estimation of the slope parameter $\beta$ which measures the effect of the explanatory variable on the response variable.[192] In our case, the slope parameter signifies the expected change in the number of clauses in data breach notification laws for each later year of the law's adoption. For instance, a positive β implies that the number of clauses grows with each additional year of delay in the law's adoption.

Returning to our research question on the quantitative effect of the year of a law's adoption and its number of clauses, we estimate the following regression equation using cross-sectional data on all fifty states (i.e., one observation per state at a snapshot in time):

$$NumberClauses = \alpha + \beta \times BaseYear + \varepsilon,$$

where *NumberClauses* and *BaseYear* are, respectively, the response and explanatory variables as described above. While there exist many statistical methods (estimators) to compute $\alpha$ and $\beta$, we specifically employ the Poisson estimator which is appropriate for response variables that represent integer counts, or simple number of occurrences of a particular outcome, such as the number of clauses within a data breach notification law that we use.[193] We applied this estimator to our data using Stata 17 software, and produced the following estimated version of equation (1):

$$NumberClauses = -457.6 + 0.227 \times BaseYear$$

Under the Poisson estimator methodology, the coefficient of interest $\beta$ can be interpreted as the "semi-elasticity" of the number of clauses with respect to the base year; that is, for one later base year the law was enacted, the number of clauses within the law is expected to change by $100*\beta$ percent on the average. Thus, the estimate of $\beta$ = +0.227 means that the number of clauses is expected to be higher by about 23% for each later year the base law was enacted.

The results of the regression analysis are standardly subject to further analysis by researchers. A major concern is whether the

191. *Id.*

192. *Id.*

193. COLIN A. CAMERON & PRAVIN K. TRIVEDI, MICROECONOMETRICS USING STATA 212-213 (Stata Press 2nd ed. 2022).

explanatory variable has a statistically significant linkage with the response variable. Statistically *insignificant* relationships are those for which the given data do not permit for a precise estimation of the $\beta$ parameter (perhaps due to small sample size, data quality, or simply the lack or a relationship), thus lending $\beta$ a large margin of error, or too-wide of a range of values it could plausibly take. If this is the case, then we cannot claim with any reasonable degree of confidence that the explanatory variable exerts influence over the response variable. However, our regression diagnostics ($\beta$'s *t-score* = +5.64; $p$ = 0.000) indicate that the slope of our equation is in fact precisely estimated, giving us a great deal of confidence that data breach notification laws adopted in later years in the dataset are indeed regulatorily stricter. Figure 13 depicts the scatter plot (with line of best fit) of the simple bivariate relationship between the number of clauses and the base year.

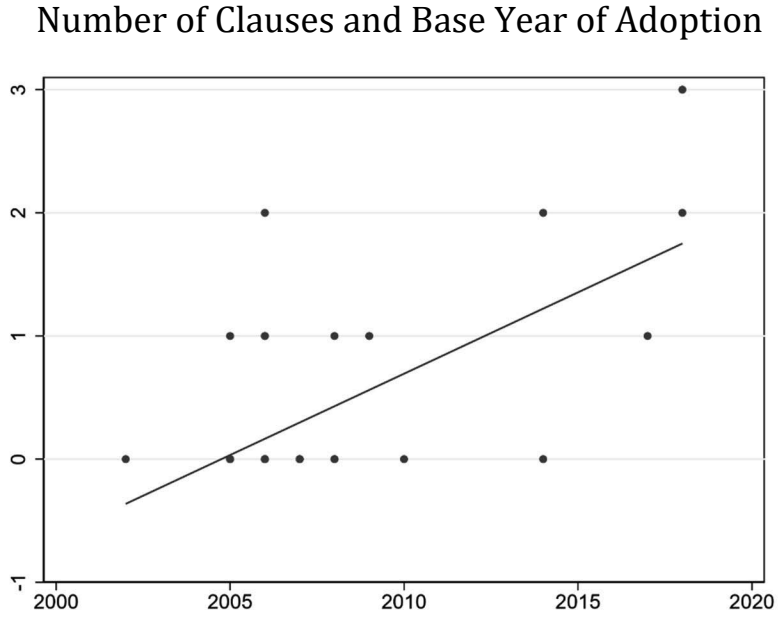



**Figure 13**[194]

194. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171 (West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732,

Next, we employ an alternative regression approach where we aggregate the cross-sectional data by state up to the national-level time series (a single entity observed over time). That is, we sum up all the clauses across all states per year, leaving us with the sequence of total clauses, by year, for the entire United States. This leaves us with seventeen years over the 2002-2018 window and thus seventeen total observations in this new dataset. We have zero observations in years where no states enacted such laws. The regression equation to be estimated now takes the form:

$$\sum NumberClauses = \alpha + \beta \times BaseYear + \gamma NumberStates + \varepsilon$$

where is the total number of observed clauses present in base laws at the U.S.-level, *BaseYear* is as defined above, and *NumberStates* represents the number of states that enacted a law at a given year. This latter variable is another important explanatory factor of the number of clauses and thus ought to be accounted for in our model if the interpretation of the coefficient of interest, $\beta$, is to be considered valid. Note that for years where no state enacted a data breach notification law, we enter the value of zero for both *NumberClauses* and *NumberStates*.

As before, positive and statistically significant value of $\beta$ here indicates that the later the base laws are enacted, the more clauses they have, independent of the number of states enacting the base law. We also use the Poisson estimator method here to estimate the coefficients of equation (3):

$$\sum NumberClauses = -540.2 + 0.268 \times BaseYear + 0.210 \times NumberStates$$

An analysis of this estimation suggests that all slopes are statistically significant ($\beta$: $p = 0.006$, $\gamma$: $p = 0.001$). As before, this result indicates a positive relationship between regulatory strictness and the year in which the base law is enacted, but from the viewpoint of the whole country. We find that for each later year of enactment, the number of clauses is higher by about 27% in the U.S. However, these results should be interpreted with caution due to small sample size. Both approaches provide some statistical evidence in support of the hypothesis that it mattered when the states decided to enact the initial data breach

---

59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess. (Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

notification law. Across the country, data breach notification legislation has exhibited a trend toward greater regulatory strictness, especially in more recent years. Figure 14 below depicts the time series plot of the number of clauses per year with the line of best (non-linear) fit.

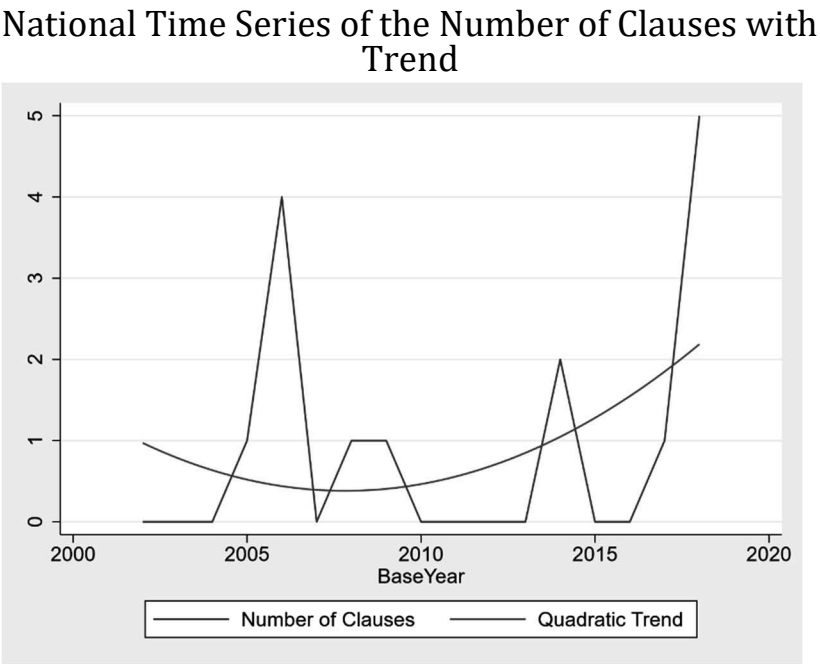



**Figure 14**[195]

195. *See* S.B. 318, 2018 Leg., Reg. Sess. (Ala. 2018); H.B. 65, 25th Leg. (Alaska 2008); S.B. 1338, 47th Leg., 2d Reg. Sess. (Ariz. 2006); S.B. 1167, 85th Leg., 2005 Reg. Sess. (Ark. 2005); CAL. CIV. CODE § 1798.29 (West 2002); H.B. 18-1128, 71st Gen. Assemb., 2d. Reg. Sess. (Colo. 2018); S.B. 650, 2005 Leg., Gen. Assem. (Conn. 2005); H.B. 116, 143rd Gen. Assemb. (Del. 2005); FL. STAT. ANN. § 501.171 (West 2024); S.B. 230, 2005 Leg., Gen. Assemb. (Ga. 2005); S.B. 2290, 23rd Leg., 2006 Reg. Sess. (Haw. 2006); S.B. 1374, 59th Leg., 2d Reg. Sess. (Idaho 2006); H.B. 1633, 94th Gen. Assemb. (Ill. 2005); S.B. 503, 2005 Leg., Reg. Sess. (Ind. 2006); S.B. 2308, 82d Gen. Assemb., 2d Reg. Sess. (Iowa 2008); S.B. 196, 2006 Leg., Reg. Sess. (Kan. 2006); H.B. 232, 2014 Leg., Reg. Sess. (Ky. 2014); S.B. 205, 2005 Leg., Reg. Sess. (La. 2005); L.D. 1671, 122d Leg., 1st Spec. Sess. (Me. 2005); H.B. 208, 2007 Leg., Reg. Sess. (Md. 2007); MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2007); S.B. 309, 2006 Leg., S.B. 309, 93rd Leg., Reg. Sess. (Mich. 2007); H.F. 2121, 84th Leg., 2005 Reg. Sess. (Minn. 2005); H.B. 489, 2010 Leg., Reg. Sess. (Miss. 2010); H.B. 62, 95th Gen. Assemb., 1st Reg. Sess. (Mo. 2009); H.B. 732, 59th Leg., Reg. Sess. (Mont. 2005); L.B. 876, 99th Leg., 2nd Reg. Sess. (Neb. 2006); S.B. 347, 73d Leg., Reg. Sess. (Nev. 2005); H.B. 1660, 2006 Leg., Reg. Sess. (N.H. 2006); A. 4001, 211th Leg., 2d Ann. Sess. (N.J. 2006); H.B. 15, 53d Leg., 1st Reg. Sess. (N.M. 2017); A.B. 4254-A, 228th Leg., Reg. Sess. (N.Y. 2005); S.B. 1048, 2005 Gen. Assemb., Reg. Sess. (N.C. 2005); S.B. 2251, 59th Leg., Reg. Sess. (N.D. 2005); H.B. 104, 126th Gen. Assemb., Reg. Sess. (Ohio 2005); H.B. 2245, 51st Leg., 2d Reg. Sess. (Okla. 2008); S.B. 583, 74th Leg. Assemb., Reg. Sess. (Or. 2007); S.B. 712, 2005 Gen. Assemb., 189th Reg. Sess. (Pa. 2005); H.B. 6191, 2005 Gen. Assemb., Reg. Sess. (R.I. 2005); S.B. 453, 2008 Leg., Reg. Sess. (S.C. 2008); S.B. 62, 93d Leg., Reg. Sess. (S.D. 2018); H.B. 2170, 104th Gen. Assemb., Reg. Sess. (Tenn. 2005); S.B. 122, 2005 Leg., 79th Reg. Sess. (Tex. 2005); S.B. 69, 56th Leg., 2006 Gen. Sess. (Utah 2006); S. 284, 2006 Gen. Assemb., 68th Biennial Sess. (Vt. 2006); H.B., 2008 Leg., Reg. Sess. (Va. 2008); S.B. 6043, 59th Leg., 2005 Reg. Sess. (Wash. 2005); S.B. 340, 2008 Leg., Reg. Sess. (W. Va. 2008); S.B. 164, 2005 Leg., Biennial Sess. (Wis. 2006); S.F. 53, 59th Leg., Gen. Sess. (Wyo. 2007).

### *C. Political Affiliations*

Our third research question examined if the party in control influenced the passage of a data breach notification law. We examined the party affiliations of both the executive level and the legislative level of the state government at the time the laws were enacted. The use of red and blue in the U.S. to distinguish between members of the conservative Republican Party and members of the liberal Democratic Party dates back two decades. Red and blue maps appeared during the 2000 election.[196] There are scholars that are critical of these maps that argue that they promote partisan polarization.[197] In 2006, Brookings Institute researchers, William Galston and Pietro Nivola, argued that the country is more purple.[198]

Quinnipiac University law professor, Jeffrey Cooper, studied red and blue states to examine how states would possibly respond to a change in the federal tax law.[199] In Congress, blue states resist federal policies related to tax reform, immigration, and marijuana; the blue states take initiative when federal policy is gridlocked, while red states pre-empt blue city antidiscrimination and environmental policies.[200] This informed our hypothesis that one of the political affiliations would dominate in enacting data breach notification laws at the state level. National policy debates are playing out in the states "resulting in a patchwork of policies and an increasingly fragmented federalism."[201] This is true for the establishment of data breach policies as well. Thus, we examined political affiliations as related to data breach notification laws.

In 2023, University of Houston political science scholar, Kristin Moore Pearson, used the political party affiliation of executive branch governors to study state-level partisan consideration in response to COVID-19.[202] We adopt the method used by University of North Florida psychology professor, Dominik Güss, and his team of researchers in

---

196. C. Dominik Güss, et al., *The Politics of COVID-19: Differences Between Blue, Purple, and Red States in COVID-19 Cases, Deaths, and Regulations*, 5 HEALTH POL'Y OPEN 2 (2023), https://doi.org/10.1016/j.hpopen.2023.100107.

197. Rémy A. Furrer, et al., *Red State, Blue State: Dichotomized Maps Mislead and Reduce Perceived Voting Influence*, 8 COGNITIVE RSCH.: PRINC. AND IMPLICATIONS 1, 2 (2023); *see also* Matt Grossmann, The Mostly Missing Results of the Republican Revolution in the States, 18, 25 (June 8, 2018) (unpublished article) (on file with Michigan State University).

198. *See* WILLIAM A. GALSTON & PIETRO S. NIVOLA, DELINEATING THE PROBLEM 6 (Brookings Inst. Press, 2006).

199. Jeffrey A. Cooper, *Red States, Blue States: Lessons from the State Death Tax Credit and the "Salt" Deduction*, 73 TAX LAWYER 1, 6, 58 (2020).

200. Shanna Rose, *State Legislatures as National Actors*, 52 POL. SYMP. (PS): POL. SCI. & POL. 436, 436 (2019).

201. *Id.*

202. Kristin Moore Pearson, State-Level Partisan Considerations In Response To The COVID-19 Pandemic (May 2023) (M.A. thesis, University of Houston) (on file with University of Houston).

2023.[203] Güss also studied the party affiliations of both the executive branch governors and state legislators to examine the political decisions in states related to confining and controlling COVID-19. If a governor's affiliation differed from the state senate and state house affiliation, these researchers labeled a state purple. These researchers' data source was Ballotpedia. In this study, we looked at the party that was in control in a state. To examine the executive branch, we noted each governor's party affiliation using the National Governors Association's database of former American governors.[204] At the legislative level, we examined which party was in control of the state senate and state house in the year that each state enacted data breach notification laws. Our data source for the legislative examination was Ballotpedia.[205]

As done in the Güss 2023 study, if the governor and state legislature political affiliations differed, we labeled the state purple. If the state house and senate affiliations differed, we also labelled that purple. Table 3 in the Appendix provides a list of the parties that were in control when each state initially enacted their data breach notification laws. Figure 15 presents the total number of states by party in control when the initial data breach law was enacted. We see that purple political affiliations dominate. Half the states were of purple control when their initial data breach notification law was enacted. In contrast to Shanna Rose's observation, a bipartisan federal government might be more likely to pass a federal data breach notification law.

Unfortunately, we cannot conduct a more fine-grained assessment of the six characteristics of data breach notification laws (i.e., whether the data breach definition includes paper and or electronic data; if personal information includes medical and/or biometric information; the number of days in reporting deadlines; and allowed delays). The problem is that each states' data breach code has changed over time. For example, what a red state adopted at the onset may not match the current characteristics of the code. Mapping the changes along with affiliations over time would be difficult but interesting future research.

---

203. Dominik C. Güss, et al., *The Politics of COVID-19: Differences between U.S. Red and Blue States in COVID-19 Regulations and Deaths*, HEALTH POL'Y OPEN, Nov. 11, 2023 at 2.

204. *Former Governors*, NAT'L GOVERNOR'S ASS'N (2024), https://www.nga.org/former-governors/.

205. *See States,* BALLOTPEDIA, https://ballotpedia.org/States#State_governments.

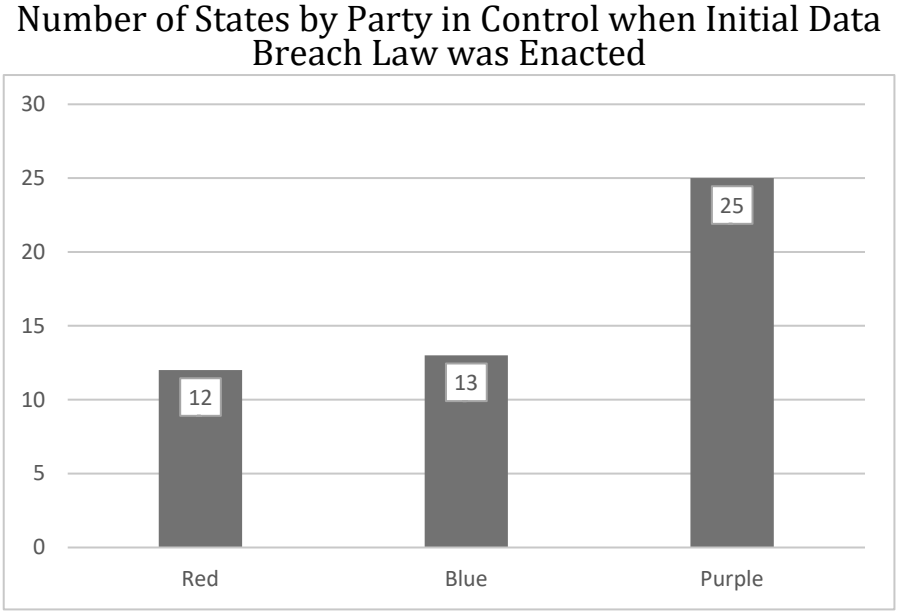



**Figure 15**[206]

## VII. BUSINESS IMPLICATIONS

The increase in data breaches is a serious threat to the protection of consumer information and has direct implications for businesses. Timely notification by businesses of the consumers' vulnerability after a data breach is essential. The advancements in Artificial Intelligence (AI) and its potential for a greater and more critical role in our daily lives, increases the concern regarding the lack of a federal data breach notification law.[207] The issue for operating American businesses is that currently each state has their own law.[208] Thus, businesses must know the varying requirements for multiple states. As mentioned with the Uber breach, some businesses have long delays in notifying their customers of a security breach.[209] Some businesses might decide to only notify customers in states with significant penalties or only notify customers in states with specific notification deadlines.[210] The data breach notifications can be costly, dependent on the number of customers impacted.[211] Notification is just one of multiple costs a business may incur

206. *Id.*

207. Mike Thomas, *14 Risks and Damgers of Artificial Intelligence (AI)*, BUILTIN (July 25, 2024), https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence.

208. *Artificial Intelligence 2024 Legislation*, NCSL, https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation (last updated Sept. 9, 2024).

209. Umang Mehta, *Issue #12: Data Breach Notifications: Why Timeliness Matters More Than Ever!*, LINKEDIN (Oct. 5, 2024), https://www.linkedin.com/pulse/issue-12-data-breach-notifications-why-timeliness-matters-umang-mehta-pqj9f/.

210. *Id.*

211. *Id.*

following a data breach.[212] These additional costs include both indirect and direct costs such as reputation damage, fines, and credit-monitoring.[213] Having to comply with different notification requirements adds to the obligation following a data breach.

The cost of addressing insider threats is the highest it has ever been, with the total average annual cost of an insider risk being $16.2 million per organization in 2023.[214] Data breaches impact both businesses and consumers. Identity fraud cost American adults $43 billion in 2023.[215] Enacting data breach notification laws can reduce the rate of identity theft.[216] The unprecedented number of data breaches in 2023 would lead to new levels of identity crimes in 2024. They also stated the lack of a uniform federal data breach notification law makes it difficult and expensive for businesses to comply.[217]

Given the advancements and ready access to artificial intelligence tools, data breaches could become even more prominent. Just as AI can assist in writing an essay or in writing software, it can be used to help facilitate data breaches. For example, AI tools can be used to create more believable phishing emails, enhance social engineering attacks, and help attackers locate system weaknesses.[218] AI assisted attacks pose a security threat to even the most robust systems.[219] As businesses face this increasing threat, a uniform federal data breach notification law would help facilitate the businesses' response to all its customers.

## VIII. CONCLUSION

The first state to pass a data breach notification law was California in 2002.[220] Then, almost twenty states passed such laws in 2005 in response to a marked increase in data breaches and several breaches that impacted millions of records. The last two states, Alabama and South Dakota, passed laws in 2018.[221] Since there are fifty different state laws,

---

212. *Id.*

213. *See* Rebecca Ong, *Mandatory Data Breach Notification: Its Role in Protecting Personal Data*, 10 J. INT'L & COMPAR. L. 87, 88–92 (2023).

214. PONEMON INSTITUTE, COST OF INSIDER RISKS GLOBAL REPORT 2023 9 (2023), https://www.dtexsystems.com/resource-ponemon-insider-risks-global-report/.

215. Christina Ianzito, *Identity Fraud Cost Americans $43 B 2023*, AARP (Apr. 10, 2024), https://www.aarp.org/money/scams-fraud/identity-fraud-report-2024/.

216. Bisogni & Asghari, *supra* note 139 at 49.

217. IDENTITY THEFT RESOURCE CENTER, 2023 BREACH REPORT, 4, 8, 19 (2023), https://www.idtheftcenter.org/publication/2023-data-breach-report/

218. Michael Hill, *5 Ways Threat Actors Can Use ChatGPT to Enhance Attacks*, CSO (Apr. 28, 2023), https://www.csoonline.com/article/575205/5-ways-threat-actors-can-use-chatgpt-to-enhance-attacks.html.

219. Dewayne Hart, *How AI-Driven Cyberattacks Will Reshape Cyber Protection*, FORBES (Mar. 19, 2024), https://www.forbes.com/councils/forbestechcouncil/2024/03/19/how-ai-driven-cyber-attacks-will-reshape-cyber-protection/.

220. Ong, *supra* note 213 at 90; *see generally* CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2023).

221. Bellamy, *supra* note 14; *see infra* Table 3.

companies must respond to data breaches in different ways. The difficulty is profound for small businesses because it is hard to prepare and manage data protection operations. It is even more costly and complicated because the data breach notification laws continue to change. This is particularly burdensome given the internet-of-things. With online and mobile commerce, companies must protect consumer data nationwide. Furthermore, with the rapid advancement of AI and increasing numbers of data breaches, there is a sense of urgency to rectify this problem.

Despite every state in the union passing its own data breach notification law, and the creation of multiple sector specific federal data breach notification laws, no global federal data breach notification law exists in the U.S. Because of the different provisions of the state laws, companies, especially small and median sized companies, have a difficult time determining what is required following a data breach. Therefore, companies need to adopt policies and procedures that will allow them to more quickly address the regulatory strictness this research found across states.

This study examined three research questions: (1) Have the laws changed from their original passage to the current content? (2) Is there a relationship between the contents of the law and when the law was passed? (3) Did the party in control influence the passage of a data breach notification law?

For the first research question, we hypothesized that the contents of the laws have changed from their original content. We found this to be true. The content of the original or base data breach notification laws has changed from their original content. Thirty-five (approximately 70%) of the fifty U.S. state laws have been amended. Sometimes amendments only involve grammatical changes or a renumbering or restructuring of state statutes. Our research revealed significant content changes have occurred. Twenty-two (i.e. 63%) of the fifty U.S. state amendments included content changes to the definition of personal information. Of the remaining states, an additional five states had amended their definition of security breach. Thus 70% of states have amended their state laws and 77% of those have amended their definition of security breach or personal information. These are significant aspects of all data breach notification laws. The pattern of continued amendments to the state data breach notification laws highlights the burden companies will continue to encounter as they must react to individual state codes and different requirements.

Our research also supports our second hypothesis that a relationship exists between the contents of the law and when the initial data breach notification law was passed. We analyzed the base laws for regulatory strictness—i.e. the presence of biometric and medical information in the definition of personal information and a specific deadline for providing the notification versus terminology such as "immediately"

or "without reasonable delay". We found a significant correlation between the law content and when the law was passed.

Because the regulatory strictness of data breach notification laws has continued to increase, policymakers should use these increasingly common components as input for creating a global federal data breach notification law. Advocates and legislators should include the following components that are common to state data breach notification laws: data breach definition; personal information definition; including medical/health information and biometrics in the definition of personal information; and including a specific reporting deadline. In addition, businesses should maintain policies that prepare them to notify individuals of a breach of personal information and to do so in approximately forty-five days.

Our third research question focused on which U.S. political party was in control when data breach legislation was passed. We found that more data breach notification legislation was passed when the parties of the executive and legislative branches differed and when the legislative houses differed. Thus, our hypothesis that one political party would dominate at the time data breach notification laws were initially enacted in a state was not supported. We surmise that an attempt to pass a federal law will be more likely to succeed when dual party control exists between the executive and legislative branches as bipartisanship and a willingness between both the red and blue members of the U.S. Congress to pass such a federal law would be required. Accordingly, bipartisan congressional action is crucial to address U.S. data breach protection comprehensively.

Why is a federal law necessary? An alternative solution would be a uniform code created by the Uniform Law Commission (ULC). However, such a uniform code would not suffice because of the long timeframe it takes for the ULC to promulgate uniform model codes. For example, the ULC drafted the Uniform Commercial Code (UCC).[222] They began the process in 1940 and did not complete the exercise until 1951.[223] Another problem with the uniform model codes is that they are not necessarily adopted by all U.S. states and when they are revised, not all states adopt the recommended revisions.[224] This has been the fate of the UCC. Nearly all states have adopted some form of it but not all

---

222. Bellamy, *supra* note 14 at 4, 9–10; *see* Andrew Wisniewsky, *Researching Uniform Laws*, UNC SCH. L. KATHRINE E. EVERETT LAW LIBR. (2024), https://library.law.unc.edu/2024/03/researching-uniform-laws/; *see also* Mary Whisner, *There Oughta Be a Law - A Model Law*, 106 LAW LIBR. J. 125, 126 (2014).

223. *Uniform Commercial Code*, UNIF. L. COMM'N, https://www.uniformlaws.org/acts/ucc (last visited Feb. 10, 2025).

224. *Uniform Laws*, CORNELL LEGAL INFORMATION INSTITUTE (LII), https://www.law.cornell.edu/uniform (last visited Feb. 10, 2025).

states.[225] So, there is not 100% uniformity. Further, the National Conference of Commissioners on Uniform State Laws (NCUSL) oversees the uniform law process.[226] Although the UCC is considered a success, nearly half the NCUSL proposals do not get adopted.[227] We believe that a uniform code for U.S. data breach protection will be on the order of a UCC in scope. If all states do not adopt a model code or recommended revisions, business owners will still have the difficulty of canvasing different laws in different states. Given the rapid advancement of AI threats to data protection, there is no time to waste. If the EU, Japan and China were able to enact laws at their federal levels as discussed in Part II of this paper, so can the U.S.

225. *Id.*
226. *Id.*
227. *Id.*

APPENDIX

**Table 1. U.S. 50 states data breach statutory definitions and notification characteristics through 2023[228]**

| **State** | **Data Breach Definition Includes Paper / Electronic (X)** | | **(Sensitive) Personal Information Includes Medical / Biometric** | | **Data Breach Notification includes reporting deadline / delay allowances** | |
|---|---|---|---|---|---|---|
| | **Paper** | **Electronic** | **Medical** | **Biometric** | **Restricted Reporting Deadline** | **Allowed Delay** |
| AL | | X | X | | 55 | Law Enforcement |
| AK | X | X | | | | Law Enforcement |
| AZ | | X | X | X | 45/45 | Law Enforcement |
| AK | | X | X | X | | Law Enforcement |
| CA | | X | X | X | | Law Enforcement |
| CO | | X | X | X | 30 | Law Enforcement |
| CT | | X | X | X | 60 | Law Enforcement |

228. *New Data Breach Notification Laws Spring 2018: What You Need to Know*, PERKINS COIE (June 12, 2018); *Data Breach Notification in the United States 2022 Report*, PRIVACY RIGHTS CLEARINGHOUSE (Jan. 27, 2023); *U.S. Data Breach Notification Law Interactive Map*, BAKERHOSTETLER, https://www.bakerlaw.com/us-data-breach-interactive-map/.

| **State** | **Data Breach Definition Includes Paper / Electronic (X)** | | **(Sensitive) Personal Information Includes Medical / Biometric** | | **Data Breach Notification includes reporting deadline / delay allowances** | |
|---|---|---|---|---|---|---|
| | **Paper** | **Electronic** | **Medical** | **Biometric** | **Restricted Reporting Deadline** | **Allowed Delay** |
| DE | | X | X | X | 60 | Law Enforcement |
| FL | | X | X | | 30 | 15 days if good cause provided. Law Enforcement |
| GA | | X | | | | Law Enforcement |
| HI | X | X | | | | Law Enforcement |
| ID | | X | | | | Law Enforcement |
| IL | | X | X | X | | Law Enforcement |
| IN | X | X | | | | |
| IA | X | X | | X | | Law Enforcement |

| **State** | **Data Breach Definition Includes Paper / Electronic (X)** | | **(Sensitive) Personal Information Includes Medical / Biometric** | | **Data Breach Notification includes reporting deadline / delay allowances** | |
|---|---|---|---|---|---|---|
| | **Paper** | **Electronic** | **Medical** | **Biometric** | **Restricted Reporting Deadline** | **Allowed Delay** |
| KS | | X | | | | Law Enforcement |
| KY | | X | | | | Law Enforcement |
| LA | | X | | X | 60 | Law Enforcement |
| ME | | X | | | 30/7 | Law Enforcement |
| MD | | X | X | X | 45/7 | Law Enforcement |
| MA | | X | | | | Law Enforcement |
| MI | | X | X | X | | Law Enforcement |
| MN | | X | | | | Law Enforcement |
| MS | | X | | | | Law Enforcement |

| **State** | **Data Breach Definition Includes Paper / Electronic (X)** | | **(Sensitive) Personal Information Includes Medical / Biometric** | | **Data Breach Notification includes reporting deadline / delay allowances** | |
|---|---|---|---|---|---|---|
| | **Paper** | **Electronic** | **Medical** | **Biometric** | **Restricted Reporting Deadline** | **Allowed Delay** |
| MO | | X | X | | | Law Enforcement |
| MT | | X | X | | | Law Enforcement |
| NE | | X | | X | | Law Enforcement |
| NV | | X | | | | Law Enforcement |
| NH | | X | | | | Law Enforcement |
| NJ | | X | | | | Law Enforcement |
| NM | | X | | X | 45 | Law Enforcement |
| NY | | X | | X | | Law Enforcement |
| NC | X | X | | X | | Law Enforcement |

| **State** | **Data Breach Definition Includes Paper / Electronic (X)** | | **(Sensitive) Personal Information Includes Medical / Biometric** | | **Data Breach Notification includes reporting deadline / delay allowances** | |
|---|---|---|---|---|---|---|
| | **Paper** | **Electronic** | **Medical** | **Biometric** | **Restricted Reporting Deadline** | **Allowed Delay** |
| ND | | X | X | | | Law Enforcement |
| OH | | X | | | 45 | Law Enforcement |
| OK | | X | | | | Law Enforcement |
| OR | | X | X | X | 45 | Law Enforcement |
| PA | | X | | | | Law Enforcement |
| RI | | X | X | | 45 | Law Enforcement |
| SC | | X | | | | Law Enforcement |
| SD | | X | X | X | 60/30 | Law Enforcement |
| TN | | X | | | 45/45 | Law Enforcement |

| **State** | **Data Breach Definition Includes Paper / Electronic (X)** | | **(Sensitive) Personal Information Includes Medical / Biometric** | | **Data Breach Notification includes reporting deadline / delay allowances** | |
|---|---|---|---|---|---|---|
| | **Paper** | **Electronic** | **Medical** | **Biometric** | **Restricted Reporting Deadline** | **Allowed Delay** |
| TX | | X | X | | 60 | Law Enforcement |
| UT | | X | | | | Law Enforcement |
| VT | | X | X | X | 45 | Law Enforcement |
| VA | | X | | | | Law Enforcement |
| WA | X | X | X | X | 30 | Law Enforcement |
| WV | | X | | | | Law Enforcement |
| WI | X | X | | X | 45 | Law Enforcement |
| WY | | X | X | X | | Law Enforcement |

**Table 2. Notification Deadlines**[229]

| Current Notification Deadline as of 2018 | | |
|---|---|---|
| Days | Number of States | Percent |
| 30 | 2 | 11.8 |
| 45 | 11 | 64.7 |
| 60 | 3 | 17.6 |
| 90 | 1 | 5.9 |

**Table 3. Partisanship Analysis**[230]

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| AL | 8-38-1 et seq. | 2018 | Red | Red | Red | Red |
| AK | CH 92 SLA 08 Now Stat. 45.48.010 et seq. | 2008 | Red | Red | Purple 10 Red/10 Blue | Red |
| AZ | Ch 232 Now 18-551 et seq. | 2006 | Blue | Red | Red | Purple |

229. Current as of 2018. COLO. REV. STAT. ANN.§ 6-1-716 (West 2018) ; DEL. CODE ANN. tit. 6, § 12B-102 (2018); LA. STAT. ANN. § 51:3074 (2018); S.D. CODIFIED LAWS §§ 22-40-20 (2018); CONN. GEN. STAT. ANN. § 36a-701(b)(1) (West 2015); ALA. CODE § 8-38-6 (2018); ARIZ. REV. STAT. § 18-545 (2016); MD. CODE ANN., COM. LAW §14-3504 (West 2015); N.M. STAT. ANN. § 57-12C-6 (West 2017); OHIO REV. CODE. ANN. §1349.19(B)(2)(West 2007);OR. REV. STAT. ANN. §646A.604 (West 2020); 11 R.I. GEN. LAWS ANN. §49.3-4 (West 2015);TENN. CODE ANN. §47-18-2107 (West 2017); VT. STAT. ANN. tit. 9 § 2435 (West 2015) ;WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2015); WIS. STAT. ANN. § 134.98 (West 2018); ME. REV. STAT. ANN. tit. 10, § 1348 (2019); CAL. HEALTH & SAFETY CODE §1280.15(b)(1) (West 2015).

230. *Security Breach Notification Chart*, PERKINS COIE (Sept. 2024), https://perkinscoie.com/sites/default/files/2024-11/Security%20Breach%20Notification%20Law%20Chart%20—%20September%202024_0.pdf; *See Gubernational and Legislative Party Control of State Government*, BALLOTPEDIA, https://ballotpedia.org/Gubernatorial_and_legislative_party_control_of_state_government.

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| AR | A.C.A. 4-110-101 et seq. | 2005 | Red | Blue | Blue | Purple |
| CA | 1798.29; 1798.82 et seq. | 2002 | Blue | Blue | Blue | Blue |
| CO | 6-1-716 | 2006 | Red | Blue | Blue | Purple |
| CT | Public Act 05-148 Now 36a-701b | 2005 | Red | Blue | Blue | Purple |
| DE | Ann. tit. 6 § 12B-101 et seq. | 2005 | Blue | Red | Blue | Purple |
| FL | 501.171 | 2014 | Red | Red | Red | Red |
| GA | 10-1-910 et seq. | 2005 | Red | Red | Red | Red |
| HI | Act 135 Now: 487N-1 et seq. | 2006 | Red | Blue | Blue | Purple |
| ID | Ch 258 Now: 28-51-104 *et seq.* | 2006 | Red | Red | Red | Red |

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| IL | Public Act 94-36 Now 8 15 ILCS 530 | 2006 | Blue | Blue | Blue | Blue |
| IN | Act 503 Now: 4-1-11 *et seq.*; 24-4.9-1 et seq. | 2005 | Blue | Red | Red | Purple |
| IA | 715C.1-2 | 2008 | Blue | Blue | Blue | Blue |
| KS | 50-7a01 et seq. | 2006 | Blue | Red | Red | Purple |
| KY | 365.732 | 2014 | Blue | Blue | Red | Purple |
| LA | 51:3071 *et seq.* *(ACT 499)* | 2005 | Blue | Blue | Blue | Blue |
| ME | 1346 *et seq.* (Public Law Ch 379) | 2005 | Blue | Blue | Blue | Blue |
| MD | 14-3501 et seq. | 2007 | Blue | Blue | Blue | Blue |
| MA | 93H § 1 *et seq.* | 2007 | Blue | Blue | Blue | Blue |
| MI | 445.63, 72 et seq. (Pub. Act. 566) | 2006 | Blue | Blue | Red | Purple |

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| MN | 325E.61 and 325E.64 (Chapter 167) | 2005 | Red | Red | Blue | Purple |
| MS | 75-24-29 | 2010 | Red | Blue | Blue | Purple |
| MO | 407.1500 | 2009 | Blue | Red | Red | Purple |
| MT | § 4 Ch 581 Now: 6-1501 *et seq*, 30-14-1701 et seq., 33-19-321 | 2005 | Blue | Purple | Blue | Blue |
| NE | § 87-801 *et seq*. | 2006 | Red | NA | Red | Red |
| NV | Ch 485 Now: § 603A.010 *et seq*., 242.183 | 2005 | Red | Blue | Red | Purple |
| NH | § 359-C:19 *et seq*. | 2006 | Blue | Red | Red | Purple |

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| NJ | § 359-C:19 *et seq*. | 2005 | Blue | Blue | Blue | Blue |
| NM | 57-12C-1 et seq. | 2017 | Red | Blue | Blue | Purple |
| NY | N.Y. Gen. Bus. Law § 899-aa; N.Y. State Tech. Law § 208 | 2005 | Red | Blue assembly | Red | Purple |
| NC | N.C. Gen. Stat. §§ 75-61, 75-65 | 2005 | Blue | Blue | Blue | Blue |
| ND | N.D. Cent. Code § 51-30-01 *et seq*. | 2005 | Red | Red | Red | Red |
| OH | Ohio Rev. Code, 1347.12, 1349.19 | 2006 | Red | Red | Red | Red |

| State | Code section | Year Enacted | Governor party affiliation | Party in control of State House | Party in control of State Senate | Decision Coded Red, Blue or Purple |
|---|---|---|---|---|---|---|
| OK | 24 Okla. Stat. § 161 *et seq*., | 2008 | Blue | Red | Purple | Purple |
| OR | Or. Rev. Stat. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626 | 2007 | Blue | Blue | Blue | Blue |
| PA | Act 94 Now: 73 Pa. Stat. § 2301 *et seq*. | 2005 | Blue | Red | Red | Purple |
| RI | Chapter 225 Now: R.I. Gen. Laws § 11-49.3-4 *et seq*. | 2005 | Red | Blue | Blue | Purple |

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| SC | S.C. Code § 39-1-90 (2008 Act No. 190, Section 7.A.) | 2008 | Red | Red | Red | Red |
| SD | S.D. CODE 22-40-20 et seq. | 2018 | Red | Red | Red | Red |
| TN | Chapter 473 Now: Tenn. Code § 47-18-2107 | 2005 | Blue | Blue | Red | Purple |
| TX | Ch 48 Now: TEX. BUS. & COM. CODE §§ 521.002, 521.053 | 2005 | Red | Red | Red | Red |

| State | Code section | Year Enacted | Governor party affiliation | Party in control of State House | Party in control of State Senate | Decision Coded Red, Blue or Purple |
|---|---|---|---|---|---|---|
| UT | Session Law Chapter 343 Now: Code §§ 13-44-101, *et seq*. | 2006 | Red | Red | Red | Red |
| VT | Act 162 9 V.S.A. §§ 2430, 2435 | 2006 | Red | Blue | Blue | Purple |
| VA | Va. Code § 18.2-186.6 | 2008 | Blue | Red | Blue | Purple |
| WA | Chapter 368 Wash. Rev. Code § 19.255.010 et seq., § 42.56.590 | 2005 | Blue | Blue | Blue | Blue |
| WV | W. VA. Code § 46A-2A-101 *et seq*. | 2008 | Blue | Blue | Blue | Blue |
| WI | Act 138 | 2006 | Blue | Red | Red | Purple |

| **State** | **Code section** | **Year Enacted** | **Governor party affiliation** | **Party in control of State House** | **Party in control of State Senate** | **Decision Coded Red, Blue or Purple** |
|---|---|---|---|---|---|---|
| | Wis. Stat. § 134.98 | | | | | |
| WY | Wyo. Stat. § 40-12-501 *et seq*. | 2007 | Blue | Red | Red | Purple |