# Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law

Charlotte A. Tschider*

*Against a backdrop of annual data breaches compromising approximately one billion global records and an average data breach cost of nearly $6 billion, the absence of clear U.S. federal strategy for data breach notification and security requirements threatens both consumer privacy and business contracting efficiency.[1] Fifty-one U.S. states and territories have created data breach notification laws and other statutes, creating a range of statutory requirements for businesses, from strict to flexible. Current state statutes provide an opportunity to create a common federal data breach notification statute, and by leveraging state statutory language in its text, a federal statute could improve security for consumers and efficiency for business while reflecting local attitudes regarding data breach notification and data protection.*



---

* © 2015 Charlotte A. Tschider. Charlotte A. Tschider holds a Master's degree in Rhetoric and Scientific and Technical Communication from the University of Minnesota, with a specialization in History and Philosophy of Science and Technology, and a Juris Doctorate from the Hamline University School of Law in St. Paul, Minnesota. Tschider owns and manages a consulting firm, Cybersimple Security LLC, and has worked as a Director of Information and Security Management and other roles in the information security and information technology field for more than fourteen years.

1. *Data Breach Industry Forecast*, EXPERIAN, http://www.experian.com/assets/data-breach/white-papers/2615-industry-forecast-experian.pdf (last visited Oct. 22, 2015).

"[N]o one can build his security upon the nobleness of another person."
—Willa Cather, Alexander's Bridge[2]

## I. INTRODUCTION

Each year, information is increasingly stored, used, and transferred fluidly for legitimate business purposes. Amid the headline-grabbing reports of state-sponsored hacking and National Security Agency surveillance lie everyday consumer transactions where consumer information is traded for goods or services: visiting a clinic, applying for a job, buying groceries with a payment card, logging onto a social networking site, or playing a game on a mobile application. Because captured personal information is collected during an initial transaction and often subsequently transferred to another business or sold for profit, the traceability of personal information is reduced, making it nearly impossible for individuals to monitor the privacy and security of their personal information. The lack of traceability thus places a heavy burden on businesses to protect this information.

Data breaches of customer personal information are becoming increasingly common, especially for U.S. businesses. Privacy Rights Clearinghouse, a nonprofit privacy advocate site reporting on U.S. data breaches, states that between 2009 and 2014, 3,058 breaches compromised over 450 million records, an increase of 53%.[3] Gemalto,

2. WILLA CATHER & ALFRED NOYES, ALEXANDER'S BRIDGE AND THE BARREL ORGAN ch. VIII (2006) (ebook).

3. *Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, http://www.privacyrights.org/data-breach/new (last visited Oct. 22, 2015).

an international digital security company, has similarly estimated worldwide compromise in 2014 of nearly 1 billion records, an increase of 49%.[4] The Ponemon Institute and IBM approximate the cost per breach at $5.9 million, or $201 per record, with breaches of at least 10,000 records at a probability of 19% over a 24-month period.[5] According to the United States Department of Health and Human Services (DHS), data breaches affecting 500 or more individuals' private health information (PHI) have increased 96% in the past four years, though many data breaches affecting PHI are not captured in any federal filing mechanism and remain unreported unless businesses are required to do so under the Health Insurance Portability and Accountability Act (HIPAA).[6] Nearly half of all Americans have had their personal information stolen in the past 12 months, and 18% of Americans have lost sensitive personal information, such as financial account numbers or PHI.[7]

In 2013 and 2014, massive data breaches dominated the news, with Target Corporation and Neiman Marcus breaches compromising hundreds of millions of credit card numbers and personal information, costing hundreds of millions in legal fees, remediation investment, and lost revenue.[8] The largest breaches reported in 2014, Home Depot and JP Morgan-Chase, compromised a total of 56 million and 83 million records, respectively, while the Anthem Inc. and Premera Blue Cross data breaches are suspected to have affected a combined 91 million health

---

4. *Gemalto Releases Findings of 2014 Breach Level Index*, GEMALTO (Feb. 12, 2015), http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-2014-Breach-Level-Index.aspx.

5. *2014 Cost of Data Breach Study: Global Analysis*, PONEMON INST. (May 5, 2014), http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

6. *Breaches Affecting 500 or More Individuals*, U.S. DEP'T HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 22, 2015); *see also* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d–6 (2012).

7. Mary Madden, *More Online Americans Say They've Experienced a Personal Data Breach*, PEW RES. CTR. (Apr. 14, 2014), http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/; Jose Pagliery, *Half of American Adults Hacked This Year*, CNNMONEY (May 28, 2014, 9:28 AM), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach.

8. *See* Samantha Sharf, *Target Shares Tumble as Retailer Reveals Cost of Data Breach*, FORBES (Aug. 5, 2014, 9:16 AM), http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/ (describing Target's data breach involving 110 million customer records at a cost of $148 million); Kara Murphy, *Neiman Marcus Continues To Pay for Security Breach*, INNOVATIVE RETAIL TECHS. (Mar. 25, 2014), http://www.retailsolutionsonline.com/doc/neiman-marcus-continues-to-pay-for-security-breach-0001 (reporting that 350,000 cards were compromised at a cost of $4.1 million and lost holiday revenue of $68 million); Keith Wagstaff, *'Worst Breach in History' Puts Data-Security Pressure on Retail Industry*, NBC NEWS (Jan. 11, 2014, 10:47 AM), http://www.cnbc.com/id/101328596#.

insurance customers.[9] Other high-profile but comparatively smaller breaches have also garnered front-page news, such as the iPhone celebrity photo scandal and the Sony Pictures breach, and at this time, there is no telling how impactful the recent United States Office of Personnel Management (OPM) government data breach will be for the 22.1 million government employees affected.[10]

Despite these record-breaking and attention-grabbing data breaches, the lack of a consistent data protection framework to protect personal information continues to create significant challenges for corporations and consumers. As a result of fragmented, sectoral federal information privacy laws, 51 states and territories began passing statutes starting in 2002, requiring specific security and privacy activities for business entities within a state, some seeking to regulate activity extraterritorially when the entity's activities affect state residents.[11] But the issues are not only local: the failure of the United States to establish a minimum baseline of protection for consumer personal information requires entities involved in interstate or international commerce to exhaust requirements in their agreements, rather than referencing governing law, leading to inefficient contracting.[12] Establishing a federal law providing a data breach notification and data protection baseline could improve interstate and international commerce through more efficient contracting, establish predictable protection and rights for consumers, facilitate global trade, and generally simplify the understanding of a complex and often technical field.

In Part I, this Author describes the origins of U.S. domestic conceptions of information privacy and data protection statutes,

---

9. Gregory S. McNeal, *Health Insurer Anthem Struck by Massive Data Breach*, FORBES (Feb. 4, 2015, 11:38 PM), http://www.forbes.com/sites/gregorymcneal/2015/02/04/massive-data-breach-at-health-insurer-anthem-reveals-social-security-numbers-and-more/; Jon Fingas, *Health Insurance Data Breach Exposes 11 Million People*, ENGADGET (Mar. 17, 2015, 7:42 PM), http://www.engadget.com/2015/03/17/premera-blue-cross-data-breach/.

10. *See* Leo Kelion, *Apple Toughens iCloud Security After Celebrity Breach*, BBC NEWS (Sept. 17, 2014), http://www.bbc.com/news/technology-29237469; *AT&T Says Some Customers Being Informed of Data Breach in August*, REUTERS (Oct. 7, 2014, 3:19 AM), http://www.reuters.com/article/2014/10/07/att-cybersecurity-idUSL3N0S208520141007; Dave Lewis, *Sony Pictures Data Breach and the PR Nightmare*, FORBES (Dec. 16, 2014, 3:00 AM), http://www.forbes.com/sites/davelewis/2014/12/16/sony-pictures-data-breach-and-the-pr-nightmare/; Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

11. *See State Data Security Breach Notification Laws*, MINTZ LEVIN, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (last modified Jan. 1, 2015).

12. *See infra* Part I.3.

including the rise of stratifying sectoral federal policy and contractual agreements.[13] These laws have resulted in fragmented data protection, a particular lack of consistency for interstate commerce, differing requirements for multifunctional corporations, and challenging interpretations for foreign corporations adequately protecting consumer data (amongst increasingly global uniformity). Part II describes state data breach notification and data protection laws including common provisions and trends across the United States. Part III describes a future proposal for a federal data breach notification and data protection law informed by state law including: applicability and scope, breach notification requirements, data protection requirements, establishment of a common federal enforcement body, preemption, and enforcement.

## II. DATA PROTECTION, INFORMATION PRIVACY, AND THE BUSINESS OF HACKING

Stealing personal information has become big business, and data breach frequency is increasing rapidly. Organized crime groups, formerly involved in illegal drug importation and money laundering, have now turned to a more reliable, safer, and more lucrative substitute in computer hacking.[14] Consumer convenience technologies such as social media, the expansion of e-commerce, and the broad use of customer data in healthcare, predictive marketing, and basic credit card transactions has only increased the variety and value of personal information to criminals.

### *A. Hacking as Big Business*

Selling personal information is now a lucrative business model, whether a business legally sells personal information, such as e-mail addresses, or a hacker steals and sells sensitive personal information, such as PHI or financial information. Selling credit card numbers nets between $.50 and $48 per card, depending on the credit line and location

---

13. While traditionally used in international data privacy law, the author uses "data protection" rather than "privacy" or "security" within this Article, as data protection combines concepts of both privacy and security by specifying requirements to protect consumer information, whether related to what information is captured, retained, destroyed, subjected to unauthorized access, or protected in a specific manner.

14. *See Masters of the Cyber-Universe*, ECONOMIST (Apr. 6, 2013), http://www.economist.com/news/special-report/21574636-chinas-state-sponsored-hackers-are-ubiquitous and-totally-unabashed-masters; *China's Cyber-Hacking: Getting Ugly*, ECONOMIST (Feb. 23, 2013), http://www.economist.com/news/leaders/21572200-if-china-wants-respect-abroad-it-must-rein-its-hackers-getting-ugly; Kenneth Rapoza, *Russia's Million Dollar Hackers*, FORBES (Apr. 24, 2012, 4:57 PM), http://www.forbes.com/sites/kenrapoza/2012/04/24/russias-millionaire-dollar-hackers/.

of the cardholder.[15] Hackers sell to black-market, bulk-card purchasers, who often use payment cards to buy merchandise and subsequently sell it at discounted prices through sites like eBay.[16] The result is highly untraceable fraud, much of it occurring globally where perpetrators cannot be identified and prosecuted due to lack of extradition treaties for computer fraud.[17] And financial information is not the only valuable type of information on the market; health information makes up nearly 44% of all breaches, can be sold for ten times the price of an individual credit card, and can be used to fraudulently create expensive insurance claims.[18]

Information privacy is not just a consumer protection issue, it is a significant economic concern. Data breaches not only affect corporations and consumers—banks, credit card issuing businesses and health insurance providers also pay for the fallout because personal information facilitates commerce. In particular, payment cards process nearly $3.5 trillion per year and 3,900 transactions each second for 78% of American households, and recent breaches have cost banking and credit card-issuing businesses hundreds of millions of dollars as a result of card reissuing and fraud coverage on payment cards.[19] Following the 2013 Target breach, almost half of U.S. banks reissued cards to avoid fraudulent charges, costing banks and issuers approximately $172

---

15. Timothy Peacock & Allan Friedman, *Automation and Disruption in Stolen Payment Card Markets*, WORKSHOP ON ECON. INFO. SECURITY 1, 5-7 (May 11, 2014), http://weis2014.econinfosec.org/papers/PeacockFriedman-WEIS2014.pdf (noting that most loss occurs quickly after the breach occurs, so slow breach notification can significantly increase fraud success, increasing reimbursement costs).

16. Deb Shinder, *What Makes Cybercrime Laws So Difficult To Enforce*, TECH REPUBLIC (Jan. 2011), http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/; *Underground Hacker Markets*, DELL SECURE WORKS (Dec. 2014), http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf.

17. Raghavendra Patidar & Lokesh Sharma, *Credit Card Fraud Detection Using Neural Network*, 1 INT'L J. SOFT COMPUTING & ENGINEERING 32 (June 2011), http://www.ijsce.org/attachments/File/NCAI2011/IJSCE_NCAI2011_025.pdf.

18. *See* Darren Boyle, *Forget Your Credit Card Details, Hackers Make 10 Times More Money from Stealing Your Medical Records—and They're Easier To Get As Hospitals' Cyber Security Is So Poor*, DAILY MAIL, http://www.dailymail.co.uk/news/article-2769109/Forget-credit-card-details-hackers-make-money-stealing-medical-records.html (last updated Sept. 25, 2014, 3:15 AM); Jessica Meyers, *Hackers Threaten Health Care Industry's Patient Records*, BOS. GLOBE (Sept. 6, 2014), http://www.bostonglobe.com/news/nation/2014/09/05/health-care-industry-ill-prepared-for-vicious-cyberthreats/ZdvDGaipJi7VSN0TogezkL/story.html. Enough personal information coupled with health insurance group and policy numbers can assist hackers in perpetuating health care fraud, or impersonating a health care facility to receive reimbursement by insurers. Insurance policy numbers are not only captured by insurers (covered entities) and hospitals, but may also be stored by other businesses, such as a person's employer. *Id.*

19. *The Business of Banking: What Every Policy Maker Needs To Know*, AM. BANKERS ASS'N 1, 27 (Dec. 2013), http://www.aba.com/Tools/Economic/Documents/Businessofbanking.pdf.

million, not including fraudulent charge coverage or increased fraud-monitoring staff.[20]

Banks are now seeking to recover these costs, alleging losses tied to reissuing cards, transaction fees, interchange fees/interest, administrative expenses, and customers.[21] In a recent class action lawsuit, banks sued Target for the cost of reissuing cards and fraud coverage, successfully defeating a motion to dismiss in December 2014 on negligence theories and under a Minnesota payment card statute. In a separate suite, Target settled a consumer class action lawsuit, paying $10 million.[22] The Home Depot and J.P. Morgan Chase breaches prompted even more card reissuing in 2014, resulting in suits from banks and consumers.[23]

State-sponsored hackers and other entities siphon global corporate income, and it is estimated that more than $445 billion of global Internet-generated revenue is stolen annually.[24] High gross domestic product

---

20. Chris Cumming, *Almost Half of U.S. Banks Are Reissuing Cards Due to Target Breach*, AM. BANKER (Dec. 2013), http://www.americanbanker.com/issues/178_248/almost-half-us-banks-are-reissuing-cards-due-to-target-breach-1064586-1.html; *Target Data Breach Cost for Banks Tops $200M*, NBC NEWS (Feb. 2014), http://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156.

21. Penny Crosman, *How Much Do Data Breaches Cost? Two Studies Attempt a Tally*, AM. BANKER (Sept. 11, 2014), http://www.americanbanker.com/issues/179_176/how-much-do-data-breaches-cost-two-studies-attempt-a-tally-1069893-1.html (describing the cost of reissuing, overall breach recovery costs, and to what degree businesses leave their financial institutions after reissuance). The cost of card reissuing can range from just under $3 per card for large banks to $11 per card for small banks.

22. *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014) (rejecting a motion to dismiss under negligence and negligence per se and Minnesota state Plastic Card Security Act provisions); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (P. Minn. 2014) (rejecting a motion to dismiss under an unjust enrichment theory); Steve Karnowski & Michelle Chapman, *Judge OKs $10 Million Settlement of Class-Action Lawsuit Over Target Corp. Data Breach*, U.S. NEWS & WORLD REP. (Mar. 19, 2015, 6:35 PM), http://www.usnews.com/news/business/articles/2015/03/19/target-proposes-to-pay-10m-to-settle-data-breach-lawsuit. Not only banks, but consumers have also sued in class action for the Target Data Breach.

23. *In re* The Home Depot, Inc., Customer Data Sec. Breach Litig., 65 F. Supp. 3d 1398 (J.P.M.L. 2014) (determining a common district for litigation regarding the Home Depot data breach); Robin Sidel, *Banks, Credit Unions Start Reissuing Cards Following Home Depot Breach*, WALL STREET J., http://www.wsj.com/articles/banks-credit-unions-start-reissuing-cards-following-home-depot-breach-1410983686 (last updated Sept. 17, 2014, 6:07 PM).

24. *See Net Losses: Estimating the Global Cost of Cybercrime*, MCAFEE 2 (2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf; Mark Clayton, *Hackers Steal 15 Percent of Money Generated by Internet, Study Estimates*, CHRISTIAN SCI. MONITOR (June 9, 2014), http://www.csmonitor.com/world/Passcode/2014/0609/Hackers-steal-15-percent-of-money-generated-by-Internet-study-estimates-video. Studies estimate that Internet shopping revenue generates between $2 and $3 trillion per year, and hackers steal around $445 billion annually, which includes not only financial crime but theft of intellectual property and confidential information. High GDP countries, like the United States are estimated to have lost .9% of GDP on average.

(GDP) countries appear to be targeted by hackers the most: these countries average an estimated loss of nearly 1% GDP for all commerce, or $151 billion annually for the United States.[25] Information privacy is a growing problem, not only for individuals, but for the global economy.

### *B. U.S. Security and Privacy Regulations*

The United States addresses privacy through a scattered set of federal regulations, Constitutional rights, contract and tort common law, and an international framework agreement.[26] Unfortunately, this federal privacy model has not sufficiently protected consumers: 51 states and territories have passed additional data breach notification and data protection laws to fill gaps within the current framework. Because federal law does not explicitly require protection of personal information or specify security or privacy requirements for nongovernmental agencies to employ (except when working on a governmental contract),[27] the dramatic rise of data breaches has prompted gap filling by way of sectoral federal law, state law, industry self-regulation, and private contracting.[28]

#### 1. Federal Banking, Healthcare, and Financial Regulations for Consumer Protection

Information including names, addresses, phone numbers, email addresses, financial account information, and corporate financial information, and others specific information types have been embedded into sectoral, industry-specific consumer laws in the healthcare industry, banking industry, and for corporate entities: HIPAA and the Health Insurance Technology for Economic and Clinical Health Act (HITECH)

---

25. *Net Losses: Estimating the Global Cost of Cybercrime*, *supra* note 24; *GDP (Current US$)*, WORLD BANK, http://data.worldbank.org/indicator/NY.GDP.MKTP (last visited Oct. 22, 2015).

26. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000) (proposing a model for information privacy in tort law). The challenge in protecting informational privacy within tort law is the lack of tangible, real injury. In this new field of tort law, real damages typically are quite low, as courts limit recovery to actual damages, rather than consequential or punitive damages, though some punitive damages may be allowed under some state laws.

27. Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541-3549 (2012).

28. *See* statutes *infra* note 29; *infra* Part I.B.3; *infra* Part II.A. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2012); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012). Consumer protection statutes outside of those for bank information and health information are similarly limited in scope, such as COPPA or FERPA, which protect children's internet privacy and educational record privacy, respectively.

for healthcare, the Gramm-Leach Bliley Act (GLBA) for banking, the Sarbanes-Oxley Act (SOX) for publicly traded businesses, and the Dodd Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) for investments.[29] Consumers also gained financial protection from Regulation Z, which caps out-of-pocket expenses for fraudulent charges at $50.[30]

These federal laws regulate big business in a variety of capacities and restrict collection and use of personal information, while requiring security controls on PHI and SPI in specific sectors.[31] Because these laws apply to limited information types in specific sectors, a variety of administrative bodies enforce these laws: the Office of the Comptroller of the Currency (OCC) enforces banking sector compliance, the Securities Exchange Committee (SEC) handles SOX and Dodd-Frank compliance, and the Department of Health and Human Services' Office for Civil Rights (OCR) supports the health sector.[32] Although protecting limited types of information based on a business sector can provide highly specialized protection, selective protection may create a false sense of security for other unprotected personal information.[33]

Because no federal law in the United States provides a broad, comprehensive set of data breach notification or data protection requirements for all businesses and consumers, other federal administrative bodies have provided catch-all protection in some

---

29. Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d–6 (2012); Health Insurance Technology for Economic and Clinical Health Act, *id.* §§ 17931-17934; Gramm-Leach Bliley Act of 1999, 15 U.S.C. §§ 6801-6809; Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2012) (codified in sections of 11, 15, 18, 28, and 29 U.S.C.); Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. §§ 1376-2223 (2012).

30. 15 U.S.C. § 1643(a)(1)(B); 12 C.F.R. § 226.12(b) (2009); Herb Weisbaum, *These Card Companies Offer Best Fraud Protection*, CNBC (Feb. 3, 2014, 6:00 AM), http://www.cnbc.com/id/101375283#; *see also* Mark Furletti, *The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Policy Considerations*, FED. RES. BANK PHIL. 5 (Oct. 2005), http://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2005/cppolicy-102005.pdf. Consumers bear costs for fraud in only two situations: when they purposefully delay reporting or do not review statements in two months. *Id.*

31. Weisbaum, *supra* note 30.

32. *Guidelines Establishing Standards for Safeguarding Customer Information*, OFF. COMPTROLLER CURRENCY (Feb. 15, 2001), http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-8.html; *Information Security and Section 404 of the Sarbanes-Oxley Act*, SANS INST. (2005), http://www.sans.org/reading-room/whitepapers/legal/information-security-section-404-sarbanes-oxley-act-1582; Gina Stevens, *Data Security Breach Notification Laws*, CONG. RES. SERV. (Apr. 10, 2012), https://www.fas.org/sgp/crs/misc/R42475.pdf.

33. Suni Munshani, *It's Not Just About Credit Card Numbers Any More*, PROTEGRITY (Aug. 2011), http://www.protegrity.com/wp-content/uploads/2011/08/protegrity-Anatomy-of-a-Data-Breach.pdf.

circumstances. Under section 5 of the Federal Trade Commission (FTC) Act, the FTC has prosecuted data breaches as unfair and deceptive trade practices, pursuing 53 actions as of August 2014.[34] Recently, the FTC testified before the Senate Committees on Judiciary and Homeland Security and Government Affairs and the Banking Subcommittee, urging heightened FTC enforcement powers and federal data protection legislation, and began suing entities it suspects of unreasonable data protection practices.[35] Other government administrative bodies have also fined businesses after data breaches, in addition to existing OCC and OCR actions.[36] In October 2014, the Federal Communications Commission (FCC) fined two telecommunications businesses (TerraCom, Inc., and YourTel America, Inc.), $10 million for storing personal information without effective security controls, a new interpretation of the Communications Act.[37]

Some industries have opted to self-govern in absence of clear federal guidance in order to improve consumer confidence and reduce fraud. In particular, global credit card issuers maintain market dominance over credit services, and have banded together to establish the Payment Card Industry (PCI) security requirements for merchants and service providers, with the primary purpose of reducing expensive

---

34. 15 U.S.C. §§ 41-58 (2012); Tripp Baltz, *Brill: FTC 'Not Looking for Perfect Security,' Only Small Number of Breach Cases*, BLOOMBERG BNA (Aug. 22, 2014), http://www.bna.com/brill-ftc-not-n17179894096/.

35. *See Testifying Before the Senate Judiciary Committee, FTC Reiterates its Support for Data Security Legislation*, FED. TRADE COMMISSION (Feb. 4, 2014), http://www.ftc.gov/news-events/press-releases/2014/02/testifying-senate-judiciary-committee-ftc-reiterates-its-support; Melissa Maalouf, *FTC Calls Again for Nationwide Data Breach Legislation and Heightened Enforcement Powers*, ZWILLGEN BLOG (Apr. 3, 2014), http://blog.zwillgen.com/2014/04/03/ftc-calls-nationwide-data-breach-legislation-heightened-enforcement-powers/; *FTC Testifies on Data Security before Senate Banking Subcommittee*, FED. TRADE COMMISSION (Feb. 3, 2014), http://www.ftc.gov/news-events/press-releases/2014/02/ftc-testifies-data-security-senate-banking-subcommittee; LabMD, Inc. v. Fed. Trade Comm'n, 776 F.3d 1275 (11th Cir. 2015); Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014); Natasha Saggar Sheth, *Scope of FTC's Authority To Enforce Cybersecurity is Questioned*, NOSSAMAN LLP (Mar. 18, 2015), http://www.nossamanlitigationadvocates.com/2015/03/scope-of-ftcs-authority-to-enforce-cybersecurity-is-questioned/.

36. *Enforcement Actions*, OFF. COMPTROLLER CURRENCY, http://www.occ.gov/topics/laws-regulations/enforcement-actions/index-enforcement-actions.html (last visited Oct. 22, 2015); *Case Examples and Resolution Agreements*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hippa/enforcement/examples/ (last visited Oct. 22, 2015).

37. Bruce A. Radke et al., *FCC Issues $10 Million Fine in Data Breach-Federal Communications Commission*, NAT'L L. REP. (Oct. 30, 2014), http://www.natlawreview.com/article/fcc-issues-10-million-fine-data-breach-federal-communications-commission.

coverage for fraudulent charges and card reissue expenses.[38] PCI requirements, PCI-DSS, require merchants and service providers of a transaction volume to validate compliance for a declared scope of business (data elements accessed, transferred, or stored, classification of the business in question, and transaction volume) in order to accept payment from certain branded credit cards.[39] Banks, then, can levy penalties for noncompliance on a retailer or service provider, sometimes in the millions of dollars for large retailers.[40] As such, businesses and consumers contracting with PCI-applicable businesses cannot always be certain, absent a more detailed investigation, that a business protects payment card information for its entire enterprise or suite of services.

2. Agreements Between Business Entities and Consumers

In recent years, global demand for specialty products and increasing costs of traditional brick-and-mortar retail stores has supercharged e-commerce, providing formerly "local" businesses international reach through Internet websites and "marketplace" programs with retail giants.[41]

In order to participate in the global marketplace, consumers regularly trade personal information, such as names, phone numbers, e-mails, credit card numbers, and a variety of other types of identification, in exchange for goods, services, social connection, or convenience.[42] In turn, businesses often collect this information to market products and services and, with "terms of use" agreements, sell or trade aggregated information.[43] While businesses often lean on "terms of use" click-wrap

---

38. Eric B. Parizo, *The History of the PCI DSS Standard: A Visual Timeline*, TECHTARGET (Nov. 2013), http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline.

39. *Payment Card Industry (PCI) Data Security Standard*, PCI SECURITY STANDARDS COUNCIL (Nov. 2013), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

40. *PCI Noncompliant Consequences*, FOCUS ON PCI, http://www.focusonpci.com/site/index.php/PCI-101/pci-noncompliant-consequences.html (last visited Oct. 22, 2015); PCI Security Standards Council, *supra* note 39, at 10.

41. Nathanial H. Clark, *Tangled in a Web: The Difficulty of Regulating Intrastate Internet Transmissions Under the Interstate Commerce Clause*, 40 MCGEORGE L. REV. 947, 955 (2009); United States v. Lopez, 514 U.S. 549 (1995) (citing Hodel v. Va. Surface Mining & Reclamation Ass'n, 452 U.S. 264, 276-77 (1981)); Perez v. United States, 402 U.S. 146, 150 (1971); Hous., E. & W. Tex. Ry. Co. v. United States, 234 U.S. 342 (1914)); *see e.g.*, *Alibaba: The World's Greatest Bazaar*, ECONOMIST (Mar. 23, 2013), http://www.economist.com/news/briefing/21573980-alibaba-trailblazing-chinese-internet-giant-will-soon-go-public-worlds-greatest-bazaar.

42. Grace Nasri, *Why Consumers Are Increasingly Willing To Trade Data for Personalization*, DIGITAL TRENDS (Dec. 10, 2012), http://www.digitaltrends.com/social-media/why-consumers-are-increasingly-willing-to-trade-data-for-personalization/.

43. Olga Kharif & Scott Moritz, *Carriers Sell Users' Tracking Data in $5.5 Billion Market*, BLOOMBERG BUS. (June 6, 2012, 1:40 AM), http://www.bloomberg.com/news/2013-06-

contracts to establish agreement between businesses and consumers, such "terms of use" do not effectively protect consumers' personal information.

The interconnected and global nature of business practices today complicates contractual relationships between consumers and businesses. Practically speaking, information required to complete a sale requires not only a physical or digital connection between the consumer and the business, but also includes third-party involvement to complete orders or support services, such as credit card companies, banks, manufacturers, logistics, and technology vendors, many dispersed across the country and globally.[44] While consumers purchasing an item or receiving a service often agree to "terms of use," consumers often have no specific knowledge regarding the treatment of their personal information. Necessarily, the burden of enforcing security and privacy terms on behalf of consumers shifts to agreement terms between the businesses collecting consumer information and third party suppliers.[45]

Unfortunately, leaving businesses to independently determine privacy requirements through contracts with consumers and third parties cannot effectively manage a complicated, international problem. While it may be valuable to explore contractual opportunities between businesses and consumers, negotiation between an individual consumer and the business in the form of "terms of use" agreements has become a bit of a farce.[46] Like any click-wrap agreement, consumers often agree without reading the terms, implicitly expecting reasonable protection for their personal information.[47] When included in "terms of use," U.S. businesses obtain permission for a variety of information uses, including tracking of buying or search habits, ability to send targeted marketing e-mail and physical mail to a consumer's address, and transfer or sale of personal information to another entity.[48] Even when a consumer reads the "terms and conditions," most agreements do not include specific security

---

06/carriers-sell-users-tracking-data-in-5-5-billion-market.html; Vicky Lai, *Is Your Data for Sale? Why Users Should Own Their Data and Be Able To Trade It*, DIGITAL POL'Y RECOMMENDATIONS, http://dcc.bitsandpicas.com/papers/Right%20to%20sell%20data.pdf (last visited Oct. 22, 2015) (describing various models for user data exchanges, including McConnachie's report on Google paying users to receive their data and Perlroth & Bilton's report on mobile apps aggregating user data). While data is often "anonymized," aggregated data points can identify a user.

44. *Credit Card Processing—CPN Overview*, CAPITAL PROCESSING NETWORK, http://cpnusa.com/overview/ (last visited Oct. 22, 2015).

45. *Id.*

46. *Id.*

47. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 623-24 (2007).

48. *Id.* at 596-97.

terms.[49] Furthermore, most agreements between consumers and businesses are contracts of adhesion: if a consumer does not want to agree to terms and conditions, the consumer must expend significant effort to read hundreds of pages of terms and conditions for competing businesses.[50] Such a time investment does not match the expected effort to purchase a low-cost consumer product or download an app on a mobile device, resulting in consumers not reading the terms at all.[51]

Terms and conditions often obliquely reference transfer of information to third parties. While broad terms for third party receipt of personal data provides flexibility to a business, such terms do not enable a consumer to monitor actual compliance. Moreover, consumers are not a party to subsequent agreements between the business and a third party where information is transferred. This translates to a loss of independent rights of recovery as a third party to the agreement between businesses, even if the consumer's personal information is mismanaged or otherwise not protected effectively by a third party.

Overall, while online "terms of use" agreements between consumers and businesses may serve an important purpose, they cannot establish a baseline for protection of personal information or solve larger international problems in trade, especially where transaction costs in negotiation increase barriers to contract formation and reduce efficiency for business transactions.[52] Ultimately, consumers have little effective bargaining power regarding how their personal information is handled by third parties, resulting in the inability to control how and the extent to which their information is protected.

---

49. *See* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences*, 70 WASH. & LEE L. REV. 341, 424 (2013) (describing privacy in terms of service as "adhesive"); Jamie Rubin, *Mobile Apps: FTC Says Vague Privacy Policies and Lack of Terms a Problem*, INFOLAWGROUP (Aug. 4, 2014), http://www.infolawgroup.com/2014/08/articles/privacy-law/mobile-apps-ftc-says-vague-privacy-policies-and-lack-of-terms-a-problem/.

50. Rubin, *supra* note 49.

51. Jessica L. Hubley, *How* Concepcion *Killed the Privacy Class Action*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 743, 744-45 (2012).

52. In international transactions, especially those including the transfer of personal information for service purposes or for United States organizations with Safe Harbor certification, how a business protects information often leads to extended negotiation over specific terms of the agreement. Having clear delineation of available negotiation boundaries by way of standard legal limits may improve overall contract negotiation efficiency for service, data transfer, SAS, or hosting agreements.

3. Agreements Between Business Entities

Contractual negotiation of information security and privacy terms also reduces efficiency, burdening commerce. Because service contracts do not benefit from "gap-filling" provisions, complex information security and privacy terms must be dickered and exhausted through negotiation, expending a significant amount of time and investment, both in selecting partners who meet a minimum security threshold and negotiating terms with those partners.[53]

When personal information loss for customers can result in financial or reputational damage to businesses, U.S. and international businesses (business customers) contracting with third-party vendors (service providers) often implement stringent and explicit privacy and security terms and conditions.[54] However, because no general U.S. data breach notification or data protection law is available for explicit reference, business customers and their service providers either negotiate privacy and security terms or service providers may agree to boilerplate language in its entirety without examining the terms or intending to fully meet the obligations (thereby failing to negotiate in good faith).[55] Indeed, legal recommendations for crafting security terms often encourage elucidation of detailed requirements rather than referencing industry standards like International Standards Organization (ISO)-27001 to improve understanding between parties of differing security maturity.[56] While the increasingly lengthy number of information security and privacy terms can lead to a "Borat" problem, when a signing party does not read the form contract yet expects different terms from the negotiation process,[57] the inclusion of these terms supports a plaintiff's

---

53. Hubley, *supra* note 51, at 733; *see* U.C.C. § 2-201 (2014); S. Treaty Doc. 98-9 (1983); A/CONF. 97/18 (1980); 19 ILM 668 (1980); 52 Fed. Reg. 6262-6280, 7737 (1987); 1489 UNTS 3; *see also* Raymond T. Nimmer, *Services Contracts: The Forgotten Sector of Commercial Law*, 26 LOY. L.A. L. REV. 725, 733-34 (1993). While gap-filling provisions exist under the UCC and the CISG, service contracts do not benefit from similarly efficient gap-filling provisions. Services contracts are beginning to dominate the global economy, as global trade now involves providing services across geographical boundaries and legal schemes. Security language is often included in such contracts, but too often business entities either accept language whole-cloth, without planning for a potential data breach (accepting the risk of a breach of contract or breach of the implied duty of good faith and fair dealing) or negotiations can be highly protracted.

54. Wayne Jansen & Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST 35-36 (Dec. 2011), http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

55. RESTATEMENT (SECOND) OF CONTRACTS § 205 (1979).

56. *Use Privacy and Security Practices and Contract Terms as Essential Criteria of Your Global Service Provider*, *supra* note 55.

57. Russell Korobkin, *The Borat Problem in Negotiation: Fraud, Assent, and the Behavioral Law and Economics of Standard Form Contracts*, 101 CAL. L. REV. 51, 78 (2013).

claim under breach of contract and may preserve indemnification in the event of data breach litigation.[58] In countries where data protection laws apply, businesses may include data provisions to ensure that other contracting parties adhere to applicable data protection law and specific security requirements, such as the E.U. model contractual clauses required for data transferred outside the E.U. geographic area.[59]

Agreement terms often have a life outside the originally negotiated contract. The business customer's terms and conditions in a first agreement frequently require a service provider to bind its third parties to the same or similar terms vis-à-vis a second agreement, causing a domino effect of reduced contract efficiency. As a practical matter, the handling of personal information often requires use of data centers, data storage services, additional backend software, hardware, infrastructure, or subcontractors. Thus, a business customer's personal information is not only affected by the parties forming a discrete business contract.[60] As a result, business customers often require service providers to bind their third parties to substantially the same provisions included in a first contract,[61] what this author calls "subprivity," a concept reflecting the long-arm application of contractual requirements to parties legally not parties to the first agreement (i.e., subcontractors and other service providers).[62] To meet subprivity terms, the service provider must

---

58. *See generally* Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, 2014 WL 10442 (2014) (describing the types of "cognizable injury" available to litigants for data breaches).

59. *EU-US Summit—Joint Statement*, EUR. COMMISSION (Mar. 26, 2014), http://europa.eu/rapid/press-release_STATEMENT-14-84_en.htm; see Decision 2001/497/EC: Set I; Decision 2004/915//EC: Set II; Decision 2010/87/EU (2014), http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm; *see also* Richard C. Owens & Francois Van Vuuren, *Outsourcing and Privacy Laws in Canada: Emerging Issues in the Regulation of Data Flows*, BLAKE, CASSELS & GRAYDON LLP (July 2007), https://www.mondaq.com/Canada/x/51642/Data+Protection+Privacy/Privacy+Law+And+Outsourcing+In+Canada+A+Current+Overview. Contracts typically are used in securing transborder data flows (e.g., data transfer of personal information). Exceptions to contractual language include agreements between countries, such as Safe Harbor certification.

60. Steve Robinson, *Security Concerns in Licensing Agreements, Part Two: Negotiating Security Provisions*, SYMANTEC, http://www.symantec.com/connect/articles/security-concerns-licensing-agreements-part-two-negotiating-security-provisions (last updated Nov. 2, 2010).

61. *See, e.g.*, *Third Party Risk Guidance on Managing Third Party Risks*, FED. BANKING L. REP. (June 6, 2008), http://www.fdic.gov/news/news/financial/2008/fil08044a.pdf. (describing forming contracts with third parties to ensure third parties follow commensurate security and privacy requirements).

62. "Subprivity" reflects the common law that a contract may not bind parties other than those party to a contract (except those signing and others listed within it that are legally tied to the entity, e.g., agents, partners, affiliates). Third parties, however, unless signing, are typically not in privity with the business customer. However, the requirement for a party in privity to contractually require a third party to follow the same obligations does the work of extending

subsequently negotiate with all applicable third parties in second agreements with terms substantially similar to the terms of the first agreement.[63] If the service provider agrees to the subprivity term while not intending to honor that term, the business customer may allege breach of the implied duty of good faith and fair dealing and breach of contract.[64] If the service provider agrees to hold its third parties to the same security and privacy terms, the service provider likely engages in protracted contract negotiations and renegotiations to ensure all of a service provider's third parties can adhere to the original business customer's terms.[65] Otherwise, the service provider likely exerts some effort in finding a replacement third party that will agree to the terms in entirety.[66] This results in a cascading and sometimes circuitous effect from a business customer and its service provider to the third parties of the service provider.[67] In particularly complex scenarios, one business arm of a customer could require the service provider to hold its third parties to the same security and privacy terms, while the customer's other business arm is a service provider for the first service provider, yet refuses to include the same precise security and privacy terms within their agreement.

While the increasingly common business concerns around third-party security and privacy accountability may prompt inclusion of security and privacy terms in an agreement, these concerns dramatically increase complexity and reduce efficiency for a service provider's contract negotiations with third parties. In an increasingly technologically inclined, global economy (where services may be outsourced, off-shored, and aggregated, as in a cloud, for cost reduction), very few service providers provide all services independently. Indeed, most service providers substantially rely on third party products and

---

privity in a way, though it does not enable a business customer to litigate against a third party. *See Privity of Contract and Third Party Rights*, L. REFORM COMMISSION (Fed. 2008), http://www.lawreform.ie/_fileupload/Reports/Report%20Privity.pdf.

63. *Guidance on Managing Risks from Third-Party Relationships*, FED. BANKING L. REP. para. 35-522 (Oct. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

64. Constance A. Anastopoulo, *Bad Faith: Building a House of Straw, Sticks, or Bricks*, 42 U. MEM. L. REV. 687, 696-700 (2012).

65. *Id.* at 701.

66. *See id.*

67. As an example, many technology companies provide base technology capabilities or data storage to businesses that support storage or processing of personal information. However, these companies also rely on business process vendors for specific services; e.g. accounting, HR, insurance, recruiting, IT consulting, payment processing; and often demand protection of personal information through these processes. Both organizations could be relying on each other as customers and as vendors, complicating contractual negotiation.

services (dwarfing the often complex construction sector), amplifying the cascading effect of requiring third party accountability, potentially *ad infinitum*.[68]

Of course, business customers have ample incentive to stipulate third party accountability through contract. In particular, business customers may have difficulty recovering under breach of contract in litigation, but may be more successful tying security and privacy term compliance with termination clauses and audit rights (e.g., periodic assessment of security controls).[69] However, unlike most litigation over payment or delivery terms, where incidental and foreseeable consequential money damages generally can be ascertained (e.g., direct loss of income or cost to cover), breach of contract for failure to meet security controls (usually determined after a data breach has occurred) could result in less foreseeable consequential damages, posing greater difficulty to calculate with "reasonable certainty"—such as reputational damage or loss of future sales.[70] When damages cannot be calculated with reasonable certainty, it is likely courts will award only nominal damages.[71] If courts are unlikely to award more than nominal damages, business customers may be more motivated to ensure terms are met

---

68. *See* Nimmer *supra* note 55. As a point of example, a supplier may contract with a third party cloud provider to store personal information of all business customers, and the present business customer wants to ensure that these cloud storage services are held to the same standards as what is fixed in the contract with the immediate service provider. Data protection requirements often pose more challenges than standard terms, including: (a) the lack of awareness of security, especially for small to medium-sized businesses; (b) a lack of capital for small to medium-sized businesses to invest in information security activities; (c) the significance of outsourced and third party activities with regard to technology; (d) the dramatic growth of the security industry, requiring substantial investments in less time, affecting all sizes of business; and (e) the fractured nature of law that could create common understanding of reasonable security, leaving contracts (and often nonsecurity experts) to agree on what "reasonable security" means within the terms of a contract.

69. *See infra*, note 74.

70. 24 WILLISTON ON CONTRACTS § 64:8 (4th ed.). *Compare* Sarah Halzack, *Home Depot and JPMorgan Are Doing Fine. Is it a Sign We're Numb to Data Breaches?*, WASH. POST, http://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/ (last updated Oct. 6, 2014, 6:31 PM), *and* Eric Chemi, *Investors Couldn't Care Less About Data Breaches*, BLOOMBERG BUS. (May 23, 2014), http://www.bloomberg.com/bw/articles/2014-05-23/why-investors-just-dont-care-about-data-breaches (describing "breach fatigue," where consumers and investors do not stop shopping at or investing with businesses post-breach), *with* Will Gangeware, *Assessing the Impact of a Privacy Breach on a Firm's Market Value*, ANTOLIN-DAVIES.COM 30 (Dec. 2013), http://www.antolin-davies.com/theses/gangewere.pdf (finding a negative reaction for investors to firms failing to fix information security flaws post-breach, evidenced by more than one breach). Further complicating the matter is that common indicators of damage, such as stock price, seem relatively impervious to data breaches, contraindicating the reasonable certainty required to successfully argue for consequential damages recovery.

71. 22 Am. Jur. 2d Damages § 17 (2015).

upfront by all parties handling personal information.[72] In many ways, protection of information is largely a preventative activity: practices do not really matter until a data breach occurs, but the occurrence of a data breach can pose difficulty in recovering damages.[73] As such, many businesses opt to include security, privacy, and associated subprivity terms in an agreement upfront, along with rights to audit and terminate, in order to hold suppliers and their third parties accountable, and to reduce the probability of a data breach occurring (from which a business customer may not fully recover pecuniary losses).[74] This is a smart move for a business customer, but it often leads to reduced efficiency and higher costs for service providers.

Modifying secondary third-party contracts to address each business customer's demands may indeed cost a service provider more, not just in terms of effort but also in actual cost. As a practical matter, most third party agreements have not expired at the moment a business customer introduces subprivity language, so service providers may need to amend or modify existing agreements with third parties. Including potentially more stringent security and privacy terms may result in changes to other previously negotiated, favorable terms (e.g., price), assuming that a third party has the capability to meet required security and privacy terms in entirety.[75] Multiplied across all business customers with whom a service provider may contract, actually adhering to subprivity terms from all business customers may prove impossible to manage, especially for service providers reliant on a large number of third parties (such as technology providers). This thereby increases the overall cost to a business customer. As a result of security and privacy term introduction and subprivity terms, all actors in this situation expend more time and energy, and price likely increases, illustrating a reduction in contract efficiency.[76]

---

72. *See, e.g.*, *Description: Risk Management Guidance*, OFF. COMPTROLLER CURRENCY (Oct. 30, 2013), http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html; Joseph Yacura, *Third Party Supplier Risk Management*, INFO. SERVS. GROUP (2013), http://www.isg-one.com/knowledgecenter/whitepapers/private/papers/White_Paper_Supply_Chain_Risk_Insurance.pdf.

73. Peter M. Watt-Morse & A. Benjamin Klaber, *Contract Corner: Cybersecurity*, NAT'L L. REV. (Oct. 16, 2014), http://www.natlawreview.com/article/contract-corner-cybersecurity.

74. *Id.*

75. Jeff Goldman, *Smaller Companies Spend 2.5 Times More on IT Security Than Larger Companies*, ESECURITY PLANET (Sept. 27, 2013), http://www.esecurityplanet.com/network-security/smaller-companies-spend-2.5-times-more-on-it-security-than-larger-companies.html. 44% of companies reported lack of a strong security posture, according to a survey in 2013. *Id.*

76. According to typical conceptions of contract law, additional terms should result in reduction of other burdens or increase in price to meet additional terms, which likely cost additional funds to implement. While in some industries, failure to meet additional terms may

While state data breach and data protection notification statutes could be referenced for local transactions, variations in statutory language across jurisdictions do not improve efficiency with regard to interstate commerce and international transactions.[77] Standardization in contractual provisions via a common U.S. federal data breach and data protection law may improve contract process efficiency and, over time, promulgate legal interpretation and administrative best practices.[78]

## III. STATE DATA BREACH NOTIFICATION AND DATA PROTECTION LAWS

As a result of the U.S. federal government's sectoral regulations with limited, embedded security and privacy provisions, states have opted to regulate broad usage of personal information for their residents.[79] Today, 51 U.S. states and territories have an information privacy regulation, ranging from solely data breach notification statutes to statutes combining data breach, data protection, and retention/disposal requirements.[80] Most states regulate corporations operating within state borders (either by reaching consumers or physical presence), requiring data breach notification within a specific time period and procedures for less expensive, broader dissemination for large breaches (e.g., television or newspaper).[81] In 2002, California was the first state to enact a data breach notification statute, but more recent statutes passed by Massachusetts and Florida reflect some of the most broadly applied and restrictive requirements to date, for example, requiring businesses to adopt a comprehensive security program if doing business with state residents and encouraging techniques to render information indecipherable, such as encryption.[82]

---

result in nonselection within an RFP, RFI, or similar process, in others there may not be an alternative service providers.

77. *See supra* Part II.

78. *See* Joshua A. T. Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1401, 1442 (2009). Under information cost theory, gap-filling provisions (default terms) could be optimal for the whole though could be inefficient for one party.

79. See *infra* Parts II and III, respectively.

80. *Security Breach Notification Laws*, NCSL, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Oct. 22, 2015).

81. *Data Breach Charts*, BAKER HOSTETLER LLP (2014), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

82. Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J. LAW & TECH. 1, 3 (2003), http://jolt.richmond.edu/v10i1/article1.pdf; Mac McMillan, *Data Breach Notification Law: Will Florida Lead?*, INFORMATIONWEEK (July 16,

The complementary state and federal system today does enable states to effectively represent the very personal needs of its residents and react to local interests and regional differences in protecting personal information.[83] However, differences in state law also create inconsistencies in the law when businesses engage in interstate commerce.[84] Purely local law, therefore, is becoming less and less common with broader use of the Internet, even in rural America.[85] Businesses large and small are emerging more frequently with major e-commerce retail marketplaces; due to consumer location, these businesses may need to comply with up to 51 data breach notification and data protection statutes and additional data protection standards for international business customers.[86] International businesses handling U.S. consumer information also face a difficult situation: how to effectively comply with 51 variations of data breach notification and data protection requirements, when the laws themselves may conflict.[87]

Likely, the extraterritorial effect of various statutes, taken together, may be difficult to manage for any entity collecting customer

---

2014, 12:15 PM), http://www.informationweek.com/healthcare/security-and-privacy/data-breach-notification-law-will-florida-lead/a/d-id/1297252; Steven A. Meyerowitz & Craig Komanecki, *The Move Towards Mandatory Encryption of Sensitive Personal Information*, 4 PRIVACY & DATA SECURITY L. 195, 195 (2009). Nevada law also requires encryption of sensitive personal information.

83. *See generally Security Breach Notification Laws*, *supra* note 80.

84. Samuel Lee, *Breach Notification Laws: Notification Requirements and Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L.J. 125, 136 (2006).

85. *See* ECONOMIST, *supra* note 41; Deborah M. Markley et al., *Case Studies of E-Commerce Activity in Rural and Small Town Business* 1 (UCED Working Paper No. 10-2007-04, 2007), http://ageconsearch.umn.edu/bitstream/112894/2/E-Commerce%20Project.pdf.

86. Reid J. Schar & Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, BLOOMBERG BNA (Aug. 9, 2013), http://www.bna.com/complicated-compliance-state-data-breach-notification-laws/; *Data Protection Laws of the World*, DLA PIPER, http://dlapiperdataprotection.com/#handbook/world-map-section (last visited Oct. 23, 2015); *International Privacy Standards*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/international-privacy-standards (last visited Oct. 23, 2015).

87. *See Global Guide to Data Breach Notifications, 2013*, WORLD L. GROUP 119 (2013), http://www.theworldlawgroup.com/wlg/Global_Data_Breach_Guide_Home.asp; Steven Bellman, et. al., *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, INFO. SOC'Y (2004), https://www8.gsb.columbia.edu/sites/decisionsciences/files/files/1172.pdf. States have implemented highly specific and relatively taxing requirements for businesses including: incorporating PCI by reference in state law (Texas), assigning retailers liability for costs during a data breach including credit monitoring and bank compensation (New Jersey, Illinois, Connecticut, Massachusetts), and imposing restrictions higher than the PCI standard (California). Because these laws generally protect a consumer residing in a state, rather than applying to entities incorporated with that state, international businesses must also comply with state laws. *Infra* note 91

information.[88] For example, if Minnesota decided to implement a statute requiring all states doing business with consumers to require 256-bit encryption (the highest known encryption standard at the time of this writing) and other states only required 128-bit encryption, within or outside a state (depending on extraterritoriality provisions), a business may have to invest in overhauling its encryption solutions to do business in Minnesota.[89] Without consistency between states, it may be cost prohibitive for many businesses to comply with individual state mandates. With zealous state legislation becoming increasingly likely and front page breach news, small businesses operating nationally without a large legal team cannot reasonably comply.[90]

### *A. Empirical Analysis of State Data Breach Notification and Data Protection Laws*

As of July 2015, U.S. state and territory legislatures have passed 51 data breach notification statutes.[91] Since 2003, a significant number of

88. *See infra* Part II.B.1; *supra* note 80.

89. *See infra* note 91. Minnesota, Nevada, and Washington have passed statutes requiring PCI compliance for payment cards. While positive for protecting payment cards, PCI is a compliance standard founded by card issuers and not a required standard for merchants or service providers. These types of provisions, while helpful for security and privacy-minded individuals, can dramatically affect interstate commerce.

90. *Id.*

91. *See Data Breach Charts*, *supra* note 81; *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 3, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; ALASKA STAT. §§ 45.48.010-090 (2014); ARIZ. REV. STAT. § 44-7501 (2014); ARK. CODE ANN. § 4-110-103 (2014); CAL. CIV. CODE § 56.06 (2014); CAL. CIV. CODE § 1798.29 (2013); CAL. CIV. CODE § 1798.82 (2013); CAL. CIV. CODE § 1798.84 (2013); COLO. REV. STAT. §§ 6-1-715 to -716 (2014); CONN. GEN. STAT. § 36a-701b (2014), amended by Conn. Legis. Serv. P.A. 15-142 (S.B. 949); CONN. GEN. STAT. § 42-471 (2014); DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2014); D.C. CODE §§ 28-3851 to -3853 (2014); FLA. STAT. §§ 501.171, 282.318 (2014); GA. CODE ANN. §§ 10-1-912, 46-5-214 (2014); 9 GUAM CODE ANN. § 48-10-80 (2013); HAW. REV. STAT. § 487N-1-7 (2014); IDAHO CODE ANN. §§ 28-51-104 to -107 (2014); 815 ILL. COMP. STAT. § 530/1 to /25 (2014); IND. CODE §§ 4-1-11-1 to -10, 24-4.9 (2014); IOWA CODE §§ 715C.1-.2 (2014); KAN. STAT. ANN. § 50-7a01 to -7a04 (2014); KY. REV. STAT. ANN. §§ 365.732, 61.931-.934 (2014); LA. REV. STAT. §§ 51:3071-:3080, 40:1300.111-.116, amended by 2015 La. Sess. Law Serv. Act 338 (H.B. 498); ME. REV. STAT. tit. 10, §§ 1346-1350 (2014); MD. CODE ANN. COM. LAW §§ 14-3501 to -3508 (2014); MD. CODE ANN. STATE GOV'T §§ 10-1301 to -1308 (2014); MASS. GEN. LAWS § 93H-1-6 (2014); 201 MASS. CODE REGS. 17.01-05 (2014); MICH. COMP. LAWS §§ 445.63, .72 (2014); MINN. STAT. §§ 325E.61, .64 (2014); MISS. CODE ANN. § 75-24-29 (2014); MO. REV. STAT. § 407.1500 (2014); MONT. CODE ANN. § 2-6-504, amended by 2015 MONT. LAWS ch. 63 (H.B. 74), (2014); NEB. REV. STAT. §§ 87-801 to -807 (2014); NEV. REV. STAT. ANN. §§ 603A.010-.040, 242.171, .181, .183, 603A.215 (2014); N.H. REV. STAT. § 359-C:19-21 (2014); N.J. STAT. ANN. § 56:8-163 (2014); N.Y. GEN. BUS. LAW § 899-aa (2014); N.Y. STATE TECH. LAW § 208 (2014); N.C. GEN. STAT. § 75-61-65, amended by 2015 N.C. Sess. Laws 2015-193 (H.B. 607), 132-1.10, 14-113.20 (2014); N.D. CENT. CODE § 51-30-01-07, amended by 2015 N.D. Laws Ch. 352 (S.B. 2214), (2014); OHIO REV. CODE ANN. §§ 1347.12, 1349.19, .191-.192, (2014); OKLA. STAT. tit. 74, § 74-3113.1 (2012); OR. REV. STAT.

statutes have also been revised to better reflect state attitudes regarding data breach notification, personal information deserving protection, and information security requirements in protecting information (*see* Figure 1).[92] In order to further investigate the details of these statutes and the subsequent prevalence of specific provisions in data breach notification statutes, all state data breach notification and related information security statutes were analyzed, to determine predominant state attitudes about protecting personal information.[93]

Analyzing a wide variety of state statutes would enable the United States Congress to determine the combination of requirements needed at a federal level, accurately reflecting local attitudes and making the best use of alternative methodologies. As former Supreme Court of the United States Justice O'Conner reiterated in *Gonzales v. Raich*, quoting Justice Brandeis's dissent in *New State 16 v. Liebmann*, "One of federalism's chief virtues . . . is that it promotes innovation by allowing . . . that a 'single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.'"[94] In such a model, Congress may look to state successes and failures in order to inform an effective federal statute. After 12 years, state breach law may have evolved to effectively inform a federal data breach notification and data protection law.[95]

---

§ 646A.600-646A.628 (2014); 73 PA. CONS. STAT. §§ 2301-2329 (2014); P.R. LAWS ANN. tit. 10 §§ 4051-4055 (2013); R.I. GEN. LAWS § 11-49.2-1 to -7 (2014), repealed by R.I. Pub. Laws ch. 15-138 (15-1 134B); S.C. CODE ANN. § 39-1-90 (2014); TENN. CODE ANN. § 47-18-2107 (2014); TEX. BUS. & COM. CODE ANN. §§ 521.002, 521.052-.053 (2014); UTAH CODE ANN. §§ 13-44-101-301 (2014); VT. STAT. ANN. tit. 9 §§ 2430, 2435 (2014); V.I. CODE ANN. §§ 2208-2209 (2014); VA. CODE ANN. §§ 18.2-186.6, 32.1-127.1:05 (2014); WASH. REV. CODE §§ 19.255.010, 42.56.590 (2014); W. VA. CODE §§ 46A-2A-101 to -105 (2014); WIS. STAT. § 134.98 (2014); WYO. STAT. ANN. §§ 40-12-501 to -509 (2014). Four states and two territories do not have a data breach notification statute: New Mexico, South Dakota, Alabama, American Samoa, and the Northern Marina Islands. States began passing laws in 2003, and the first official data breach law was passed by California. Kentucky passed the most recent data breach law in 2014. Many states have subsequently passed multiple amendments to these statutes.

92. *See Security Breach Notification Laws*, *supra* note 80.

93. This study was conducted using data breach notification and data protection statutory language available at the time of study. Since the study, eight states have updated their statutes and thirty-two are considering updates. The recently updated statutes have primarily added to previous statutory language, increasing the stringency of requirements, and have not dramatically altered the findings of this study. *2015 Security Breach Legislation*, NAT'L CONF. ST. LEGISLATURES (June 11, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx.

94. Gonzales v. Raich, 545 U.S. 1, 42 (2005) (quoting Justice Brandeis' dissent in *New State Ice v. Liebmann*).

95. *See generally* Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693 (2007) (describing the complex pattern of federal and state laws, and

In order to determine which contents should be included in a federal data breach notification and data protection law, the author divided each of the 51 statutes (and associated related statutes) into their individual statutory requirements. The statutory subsets were grouped into requirements that affected the *application* of the statute and requirements that affected the *enforcement* of the statute.[96] Each requirement was assigned a value: restrictive, moderate, or flexible, based on the impact on an entity following such a requirement (restrictive for business would be most protective for personal information).[97] As an example, specific requirements, such as required contents for a data breach notification, would be comparatively more restrictive than notification content requirements. After these requirements were assessed, requirements were weighted for overall expected impact to businesses, based on language. The actual frequency of enforcement via litigation or documented fines was not evaluated across all states, though in practice, heavy enforcement by a state Attorney General, for example, could make a statute more restrictive, and vice-versa.

### *B. Research Outcomes*

Overall, to some degree, statutory ratings matched current perceptions of more restrictive statutes. The eleven most restrictive states were North Carolina, California, Massachusetts, Louisiana, Florida, Ohio, Alabama, New York, Maryland, Vermont, and Oregon.[98]

---

advocating that more time needs to pass before the United States determines its approach to privacy and data breach laws).

96. The application requirements included (with weighting, total of five): (a) the definition type (1) (for example the category of what information was protected [personal information, personally identifiable information, etc.]); (b) the definition details (1) (such as the type of information covered under such a definition); (c) to which entities the statutes applies (.5) (such everyone storing personal information or only data collectors); (d) whether the statute had extraterritorial reach (1); (e) if exceptions existed for statutory application (.5) (such as encrypting personal information, the so-called encryption "safe harbor"); and (f) whether the statute was preempted by federal law or industry practice (1). The enforcement requirements included (with weighting, total of five): (a) whether substitute notice (other than direct personal notice) was required (1); (b) when an entity must notify (.5); (c) contents of such notification (.5); (d) whether additional requirements were required to protect the information (1) (security requirements); (e) the dollar value of penalties for failure to follow the statute (.5); (f) whether a private cause of action is allowed (.5); (g) whether future damages are recoverable (.5); and (h) whether the AG or similar state agency has explicit rights to prosecute (.5). Each of these values was then multiplied by the value for restrictiveness (Flexible, 1, Moderate, 2, Restrictive, 3).

97. Restrictive, moderate, and flexible were categories based on weighted scores for application and enforcement requirements.

98. *See* statutes *supra* note 91.

Comparatively, Mississippi, Nebraska, Arizona, Washington, D.C., South Carolina, Hawaii, North Dakota, Virginia, Wyoming, Colorado, and Guam were the most flexible.[99] Over time and with some states amending their statutes to a more restrictive version, overall balance shifted from more flexible to more restrictive data breach notification and data protection requirements, with 2009 being a pivotal year (*See* Figure 2).[100]

1. Entities, Extraterritoriality, and Information Covered

Regulated business entities across statutes varied tremendously, from information brokers to information collectors, to any entity owning or licensing personal information, or, broadly, anyone storing personal information.[101] Around 31% of statutes employed highly specific language, limiting statutes to nongovernment organizations incorporated or doing business in the state, while 57% employed broader language, including any organization handling personal information of state residents or including commercial and noncommercial entities, as well as state agencies.[102] This definition of statutory application extended to extraterritorial effect: after 2007, extraterritorial provisions increased dramatically, to 54% of statutes adopting overt extraterritorial provisions.[103]

Despite broad and increasing application of statutes, however, the breadth of information covered by the majority of states did not increase as dramatically. Forty-seven percent of statutes used just six information

| **State** | NC | CA | MA | LA | FL | OH | AL | NY | MD | VT & OR |
|---|---|---|---|---|---|---|---|---|---|---|
| **Rank** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **Value** | 24.5 | 24 | 23.5 | 23 | 23 | 22.5 | 22.5 | 21.5 | 21.5 | 21 |

99. *See* statues *supra* note 91. Note: North Dakota and Wyoming did recently revise data breach notification and data protection statutory language, which likely increased their relative restrictiveness.

| **State** | MS | NE | AZ | DC & SC | HI, ND, VI, & WY | CO & GU |
|---|---|---|---|---|---|---|
| **Rank** | 51 | 50 | 49 | 48 & 47 | 46, 45, 44 & 43 | 42 & 41 |
| **Value** | 11.5 | 12.5 | 13 | 13.5 | 14.5 | 15.5 |

100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*

types or less, while 53% included more than six information types.[104] The most common information types, seen in every statute, included financial information such as credit card, debit card, and financial account numbers (combined with required security passcodes, PINs, or access codes); social security numbers; and state identification numbers.[105] Health information, health insurance, and biometric information were classified in a moderate number of states, suggesting that these information types have emerged as sources of consumer concern or potential fraud (*See* Figure 3).[106]

Statutes increasingly include data protection requirements, as well. While early adoption of data breach notification statutes did not include data protection requirements, such as employing reasonable security procedures or limiting data retention timeframes, this trend has changed significantly in the past three years.[107] Today, 55% of all data breach statutes passed since 2005 include multiple data protection requirements, and 14% have at least one.[108] Since 2012, nine of thirteen statutes passed have multiple data protection requirements (*See* Figure 4).[109]

2. Exemption, Preemption, and Waivers

Exemption, preemption, and waiver provisions illustrate the degree to which an entity otherwise required to comply can effectively avoid statutory requirements. Exemption provisions in data breach notification statutes included other federal statutes, such as HIPAA, GLBA, and a variety of general federal guidelines.[110] Most states employ the most flexible of exemption provisions, providing that an entity managing its own internal information security policy that included data breach procedures for personal information could effectively comply, as long as the entity met the notification timing requirements of the statute.[111]

States also make ample use of a data manipulation safe harbor. All of the statutes reference a safe harbor for manipulated data, whether referencing actual encryption technologies or other methods rendering information partially or completely unreadable, such as redaction, and

104. *Id.* Information types were counted twice for statutes that included language like "credit cards with or without passcodes."

105. *See* statutes cited *supra* note 91.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

presumably including obfuscation, tokenization, or masking.[112] Because encryption may be expensive or impactful for technology performance, many states have adapted statutes to include other forms of limiting data exposure.[113] If a data breach occurs, but the information breached is rendered unreadable, organizations are not obligated to notify residents, assuming the likelihood of misuse is low.[114]

States vary to what degree waivers were deemed voidable and unenforceable. Waivers, as in any statutory context, typically involve contractual agreements to waive some right an individual is otherwise entitled to enforce. Likely due to a concern about consumers not reading terms of use and other online contracts used to provision services, many states incorporate language limiting the use of waivers to disclaim organization breach responsibilities.[115] However, only 37% of statutes today include explicit no-waiver language, and the use of statutes that do include such language has decreased over the past three years.[116]

3. Notice Timing, Extra Notice, Details, and Substitution

When entities have not successfully avoided compliance with a data security breach statute, they must actually notify individuals impacted by a data security breach.[117] However, the speed of the communication can matter very much for a consumer. Because fraudsters and identity thieves know a limited window exists before someone discovers the issue, most criminals act quickly to maximize gains. Most statutes, however, employ flexible language subject to interpretation, the most popular being "without unreasonable delay" (76% of statutes), while other states opt to specify time requirements (17%).[118]

The contents of data breach notifications, along with the method of delivery, can play a significant role in whether consumers receive helpful information from an entity and the likelihood of that communication reaching a resident of that state. When required, content of such communications often includes a description of the data breach, contact

---

112. *See* statutes cited *supra* note 91; *see generally* Greg Sohulz, *Top 10 Ways To Secure Your Stored Data*, COMPUTERWORLD (Aug. 3, 2006), https://www.computerworld.com/article/2546352/data-center/top-10-ways-to-secure-your-stored-data.html (describing methods of protecting data).

113. Statutes cited *supra* note 91.

114. *See Security Breach Notification Laws*, *supra* note 81.

115. *See* statutes cited *supra* note 91.

116. *See* statutes cited *supra* note 91.

117. *See* Gina Stevens, *Data Security Breach Notification Laws*, CONG. RES. SERV. (Apr. 10, 2012), https://www.fas.org/sgp/crs/misc/R42475.pdf.

118. *See* statutes cited *supra* note 91; *see also Security Breach Notification Laws supra* note 81.

information for the entity breached, what information it stores about the person affected, and contact information for the FTC, the state Attorney General, or consumer credit reporting agencies.[119] Despite the helpfulness of the information, the vast majority of statutes do not require specific content in notifications.[120]

When large breaches affect many customers, most states allow substitute notice to communicate a data breach with residents.[121] If over a certain threshold of notification, cost, or residents affected is met, organizations do not need to communicate directly with residents but instead typically must e-mail residents if an e-mail address is available, conspicuously post a notice on a website, and (or, depending on the statute) notify major local or statewide media.[122] These steps reduce financial burden for organizations by using common communication channels. However, residents may not know if they individually have been affected by a breach. About 65% of statutes set a cost limit at around $150,000.[123]

Some statutes also require an entity to notify the Attorney General's office, the major consumer credit reporting agencies, or other state agencies.[124] For statutes that do require notification to the Attorney General or consumer credit reporting agencies, often a threshold must be met, most commonly, 1,000 or more residents affected.[125] Over time, required reporting to consumer credit reporting agencies has become increasingly common at around 53%, while Attorney General notice has decreased in popularity, at 37%.[126]

4. Penalties and Private Action

Penalties and private action illustrate the push and pull between Attorney General suits and associated penalties with a consumer's right to recover for injury sustained. Across all statutes, a wide variety of penalties are imposed, and often no penalty amount is specified.[127] The wide variety of penalties shows the significantly divergent status of data breach notification statutes: incorporation of data breach notification statutes into existing consumer fraud statutes versus creation of data

119. *See* statutes cited *supra* note 91.
120. Statutes cited *supra* note 91.
121. Statutes cited *supra* note 91.
122. Statutes cited *supra* note 91.
123. Statutes cited *supra* note 91.
124. *See Security Breach Notification Laws supra* note 81; statutes cited *supra* note 91.
125. Statutes cited *supra* note 91.
126. Statutes cited *supra* note 91.
127. Statutes cited *supra* note 91.

breach notification-specific penalties for noncompliance.[128] Private action likewise occupies the spectrum of options. While before 2013 only 17% of statutes permitted a private right of action, this figure has increased in recent revisions (*See* Figure 5).[129] Most statutes specifically limit rights to the Attorney General's prosecutorial power.[130]

## IV. RECOMMENDATIONS FOR FEDERAL LAW PROVISIONS

As global commerce increases, personal information is affected by broader, interdependent relationships, rather than strictly local activities.[131] Because personal information is collected, transferred, and held by commercial businesses, at the request of the customer to provision services, often resulting in data transfers, a federal statute should regulate all businesses involving consumer personal information to effectively preserve customer choice and control with respect to their information, to drive contract efficiency, and to facilitate international trade.

### *A. Applicability, Administration, and Preemption*

Several privacy scholars have advocated for a federal data breach notification and data protection statute (or equivalent consistent state statutes), and with good reason: a generally applicable federal statute will improve customer trust in businesses, identify clear expectations for corporate security and privacy requirements in interstate commerce, and improve efficiency for business relationships domestically and internationally.[132] Given that existing regulations provide higher security controls for specific industries, a federal statute could establish a baseline for data protection, yet preserve higher levels of federal protection and inform oversight for health care and banking sector customers through preemption provisions for HIPAA/HITECH and GLBA.[133]

Despite preemption of HIPAA/HITECH and GLBA over a general federal data breach notification and data protection law, the general

---

128. Statutes cited *supra* note 91.
129. Statutes cited *supra* note 91.
130. Statutes cited *supra* note 91.
131. *See* ECONOMIST, *supra* note 41.
132. *See, e.g.*, Kenneth M. Siegal, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN ST. L. REV. 779 (2007); Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355 (2006); Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395 (2014).
133. Picanso, *supra* note 132.

federal statute should also be inclusive of information types such as banking or PHI, which are transferred or stored by entities not regulated by the OCR or the OCC.[134] The general federal statute would then apply to information dominantly protected across state legislatures, including payment card information, financial information, social security numbers, state ID and passport numbers, as well as emerging areas of concern such as private health and medical information.[135]

The statutory language should also designate a primary governing body for data protection. While multiple agencies manage specific sectors, the federal statute should include a primary responsible agency, most likely the FTC, as the group has brought actions against many breached entities in the past three years and has broad rule-making authority across sectors, except where preemption applies.[136] While other agencies have a stake in receiving information about data breaches, such as the DHS and the SEC, the FTC should have primary management responsibility for activities surrounding data breaches. In addition to previous experience in this space, the FTC is associated with all businesses in the United States, exhibiting broad rule-making authority and regulatory power, enabling it to selectively audit businesses, drive statutory compliance, and create a standard fine scheme.[137] When breaches overlap with previously regulated sectors, the FTC can effectively partner with other federal agencies and with state agencies and state attorney generals, as necessary, to enforce its directives for businesses incorporated in that state and assist with investigations.[138]

Though state governments have largely developed data breach notification and some data protection laws, the federal statute should preempt state laws with regard to interstate commerce. While states may advocate for independent authority, state laws illustrate a broad range of protection from flexible to restrictive, and adding an additional statute

134. *See* statutes cited *supra* note 29.

135. *See supra* Part II.B.1.

136. *See* Baltz, *supra* note 34.

137. *See* Stevens, *supra* note 32; Radke, *supra* note 37.

138. *Statement of Work: Form Development Project, Designing Easy-to-Understand Consumer Financial Privacy Notices*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/model_form_statement_of_work.pdf (last visited Oct. 28, 2015) (describing a joint project between the SEC, OCC, FTC, and others to create easy to understand privacy notices—other collaboration will surely be necessary with regard to data breach notification and data protection); Jessica Rich, *Working Together to Protect Consumers*, FED. TRADE COMMISSION (May 19, 2014), https://www.ftc.gov/system/files/documents/public_statements/310541/140519naggremarks.pdf.

without state preemption only further complicates compliance.[139] States, of course, could continue to regulate state agencies and purely local business operations within their borders with more burdensome requirements, if they so choose. However, without clear preemption of state laws, creating a harmonized set of requirements for businesses to comply would be nearly impossible. Though significant strides could be gained by incorporating explicit state law language and trends to reflect local attitudes, the federal statute should occupy.

### *B. Data Protection Requirements*

Ultimately, the best data breach notifications are those that never need to be sent. While most state statutes and proposed federal laws have focused on data breach notification for consumers, states have also begun to recognize the importance of enforcing appropriate data protection measures.[140] Establishing data protection standards is critical not only in preventing breaches, but also may be important to determine culpability for future fines and/or class action lawsuits. Indeed, the FTC is already assessing the reasonability of security requirements employed to protect data after a data breach.[141] While a federal statute should broadly reference "reasonable security measures and retention of personal information" commensurate with information type and legitimate consumer and business needs, the FTC has an opportunity to create or adopt specific data protection standards.[142] These standards can be used for interpretive purposes in a court of law and help businesses understand how to implement risk management programs. By partnering with other internal organizations, such as the National Institute of Standards and Technology (NIST), which has already established a robust collection of security guidelines, the FTC can provide concrete direction to businesses, reducing uncertainty and protecting data more consistently.[143] While the

---

139. *See* discussion *infra* Part II; Allison Grande, *AG Fights Push for Federal Data Breach Law*, LAW360 (Feb. 5, 2015, 11:17 PM), http://www.law360.com/articles/618003/ill-ag-fights-push-for-federal-data-breach-law. While state AGs may advocate narrow preemption, not preempting more stringent requirements will fail to simplify the patchwork of breach notification laws.

140. Grande, *supra* note 139.

141. Travis D. Breaux & David L. Baumer, *Legally "Reasonable" Security Requirements: A 10-year FTC Retrospective*, 30 COMPUTERS & SECURITY 178 (2011), http://www.cs.cmu.edu/~breaux/publications/tdbreaux-cose10.pdf.

142. Joel Brenner, *An Emerging Standard of Care in Cybersecurity*, JOELBRENNER.COM, http://joelbrenner.com/an-emerging-standard-of-care-in-cybersecurity/ (last visited Oct. 23, 2015).

143. *Cybersecurity Framework*, NIST, http://www.nist.gov/cyberframework/ (last updated July 1, 2015).

implementation of data protection standards will not eliminate the need for data breach notification, it should enable businesses to better protect themselves and consumers.[144]

Having clear data protection standards will dramatically reduce uncertainty for consumers and business, as standard data protection requirements will be articulated and required for implementation, preferably in a phased approach for small businesses, some of which could apply for exemptions based on the type of business and associated risk of information loss. Over time the FTC could conduct risk assessments and site visits following consumer complaints or provide certification to specific qualified assessors, similar to the Qualified Security Assessor program used by the PCI.[145] This will enable the FTC to monitor the progress of businesses employing information security tools and privacy principles in their organizations without heavy operational involvement. Other provisions should establish that where there is overlap with more stringent industry best practices, such as PCI-DSS v3 or ISO-27001 (both considered strong frameworks for data protection), businesses may maintain certification for a specific business scope, rather than employing lesser baseline standards under the statute.[146]

### *C. Breach Notification*

A federal data breach notification statute should equally apply to all parties handling personal information, including information transferred outside of a U.S. jurisdiction, and require the same data protection standards be implemented and that third parties notify primary business data owners or licensees if a breach has occurred.[147] This requirement will enable the United States to establish similar baselines across markets, similar to the E.U.[148] In addition, it should require communication between a third party and their service provider, while simultaneously holding a third party to the same terms as the primary

144. Jordan McCarthy, *Make Hacker's Jobs Harder*, SLATE (Mar. 16, 2015, 9:27 AM), http://www.slate.com/articles/technology/safety_net/2015/03/how_to_make_it_harder_for_hackers_to_assemble_your_personal_information.html. While no business can be fully secure without halting business operation, businesses can certainly become more secure, reducing the effectiveness of the hacking enterprise.

145. *Become a Qualified Security Assessor (QSA)*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/approved_companies_providers/become_qsa.php (last visited Oct. 23, 2015).

146. Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 557-559 (2010).

147. *See* statutes cited *supra* note 91.

148. *See* statutes cited *supra* note 91.

service provider, made clear through a common U.S. federal law, eliminating complex subprivity contracting requirements and simplifying contract language.[149]

Of all requirements, notification speed is most critical, due to the time-sensitive nature of some types of fraud. Because of the importance of timely response, a federal statute should require businesses to disclose to the FTC and the DHS's National Cybersecurity and Communications Integration Center, as soon as they are reasonably certain a breach has occurred, in line with President Obama's thirty-day notification recommendation.[150] While generally states have not required notification to government agencies, the FTC, as a regulator of trade in the United States and responsible for ensuring consumer protection without overburdening businesses,[151] should receive timely notification, in order to effectively assist businesses during a data breach and reduce impact to consumers and businesses affected by fraud.[152] With timely notification, the FTC, then, can broker conversations with card issuers or other entities, as well as monitor the timeliness and reasonableness of actions related to breach notification and subsequent remediation activities.

Notification to consumers should also be timely and complete, in coordination with the FTC and other administrative agencies. Following a data breach, consistent with most state laws, the notification to

---

149. *See* Part I.B.3.

150. *See* Clayton, *supra* note 24; Maria Korolov, *Obama Proposes New 30-Day Data Breach Notification Law*, CSO (Jan. 2015), http://www.csoonline.com/article/2868096/data-protection/obama-proposes-new-30-day-data-breach-notification-law.html; *Securing Cyberspace—President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*, WHITE HOUSE (Jan. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat; *FBI, NSA, and US Secret Service Investigate Hacks at Five US Banks*, MASS COMMS., http://masscommgroup.com/secutiry/fbi-nsa-and-us-secret-service-investigate-hacks-at-five-us-banks/ (last visited Sept. 15, 2015). Most businesses today are encouraged to share any details with the FBI and the Secret Service may investigate. The creation of a new cybersecurity communications center should enable more effective root cause analysis and correlation of cyberattacks, aiding the U.S. government in assisting consumers, business, and inform global data protection conversations. While today, suspicions are on the rise regarding the collection and monitoring of public businesses under President Obama's proposed data breach law, basic information sharing should be required in order to better prosecute U.S. citizens and effectively estimate the impact breaches have on U.S. business, hopefully enabling effective extradition agreements and an eventual cybersecurity convention.

151. *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc (last visited Oct. 23, 2015).

152. *Data Security*, NAFCU (July 2015), http://www.nafcu.org/datasecurity/; *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, SEC. EXCHANGE COMMISSION (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (urging corporations to disclose information in a timely, comprehensive, and accurate manner, in line with federal securities laws, implying that cybersecurity is an important topic, relevant to an investor).

consumers should include a common method of notification based on the number of records compromised, and all notifications should include the nature of the breach, when the breach likely occurred, the extent of the breach, and what information may have been affected. While states have not universally adopted notification contents, a federal statute should establish consistency for the benefit of consumers receiving notification.[153]

### *D. Enforcement*

Under the federal breach notification statute, the FTC should be given latitude to fine businesses where necessary or bring a legal action to prosecute unfair or deceptive trade practices through Congressional Act rather than justification under the "unfairness doctrine."[154] While today, the FTC has prosecuted a wide variety of data breaches, it should work closely with partner administrative agencies to determine appropriate industries, timing, and methods for holding entities accountable.[155] A federal data breach statute should enable clear demarcation between the FTC and other agencies and clearly describe FTC responsibilities in relation to data breaches and data protection activities.

In addition to FTC legal action, the federal statute should not prohibit breach of contract actions (which involve private party agreements) or class action lawsuits, provided a class meets federal class certification requirements. While class action lawsuits have been criticized due to the sizable cost to a business with relative small awards to individuals,[156] the benefits of class action lawsuits may provide recovery to consumers who otherwise may not be able to afford legal fees, while simultaneously incentivizing businesses to follow the federal statute.[157] Additionally, class action lawsuits enable consolidation of similar actions against a common entity, necessary when most data breaches involve hundreds, thousands, or millions of records.[158]

---

153. *See* statutes cited *supra* note 91.

154. Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, ABA (Aug. 20, 2007), http://www.americanbar.org/content/dam/aba/publications/antitrust_law/20120911_at12911_materials.authcheckdam.pdf.

155. *Id.*

156. Charles E. Reuther, *Class Actions and the Quest for a Fair Resolution in Mass Tort Litigation*, 2011 N.J. LAW 25, 27 (2011); Gina Stevens, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, CONGRESSIONAL RES. SERV. 1, 7 (Sept. 2014), https://www.fas.org/sgp/crs/misc/R43723.pdf. The FTC pursued its more than fifty data security enforcement actions in 2014. *Id.*

157. *Id.* at 26.

158. *Id.* at 25-26.

The federal statute should, however, bar individual tort actions, which are not practical for individual citizens or businesses in a post breach age. In comparison to consolidated class action lawsuits, individual awards may be very small, while simultaneously creating a huge volume of individual suits, given the impact of a single breach.[159] Overall, class action lawsuits and breach of contract actions present more efficient options, yet may provide recovery for damages, deterring illegal behavior under the federal statute.

## V. CONCLUSION

The overwhelming frequency of data breaches impacting U.S. consumers' personal information signals a clear need for improvements in U.S. data breach notification and data protection law. State laws have proven significantly helpful in establishing specific contents for a proposed federal law, and have enabled the United States to reflect local preferences and modern trends in data breach notification and data protection policy.

By adopting a semi sectoral federal approach to U.S. data protection laws, the United States is likely to reduce data breaches and their damaging effect on consumers and business by creating consistent, predictable, and attainable security goals. Furthermore, with predictable standards, businesses in the United States can more efficiently manage interstate and international business relationships and more confidently deliver services. Modern commerce requires a change in approach, a change the United States may finally be ready to make.

159. *See Data Security*, *supra* note 152. *See generally* Timothy H. Madden, *Data Breach Class Action Litigation—A Tough Road for Plaintiffs*, 55 BOSTON J. 27 (2011) (describing the difficulties of effectively litigating as plaintiffs for data breach class action litigation). Though class actions may be difficult for some parties, such as individual consumers, other parties may have more success, such as banks litigating on the basis of replacement fees and fraud coverage, much of which may not be effectively compensating through an FTC fine structure.

EXHIBIT: TABLES AND CHARTS

Figure 1: Data Breach Notification Laws[160]

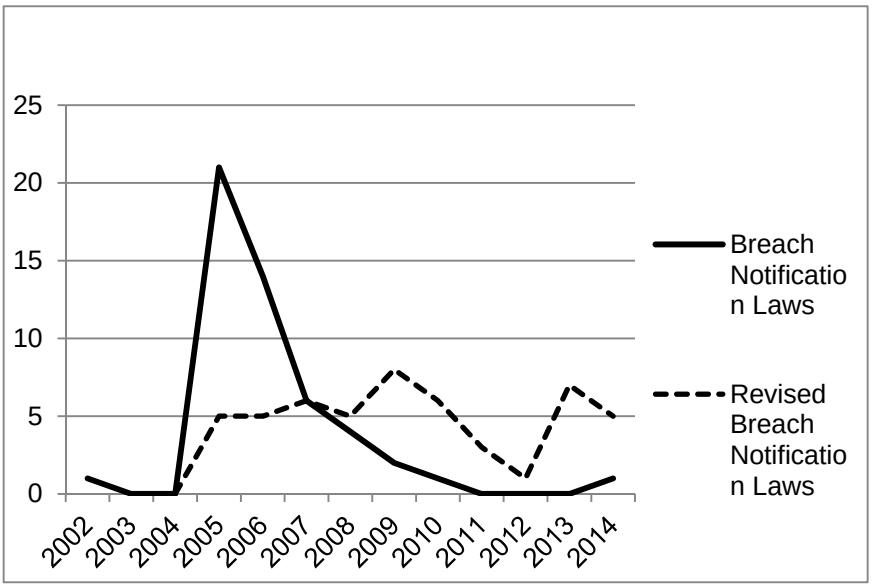



Figure 2: Overall Restrictiveness of Data Breach Notification Statutes by Year of Passage[161]

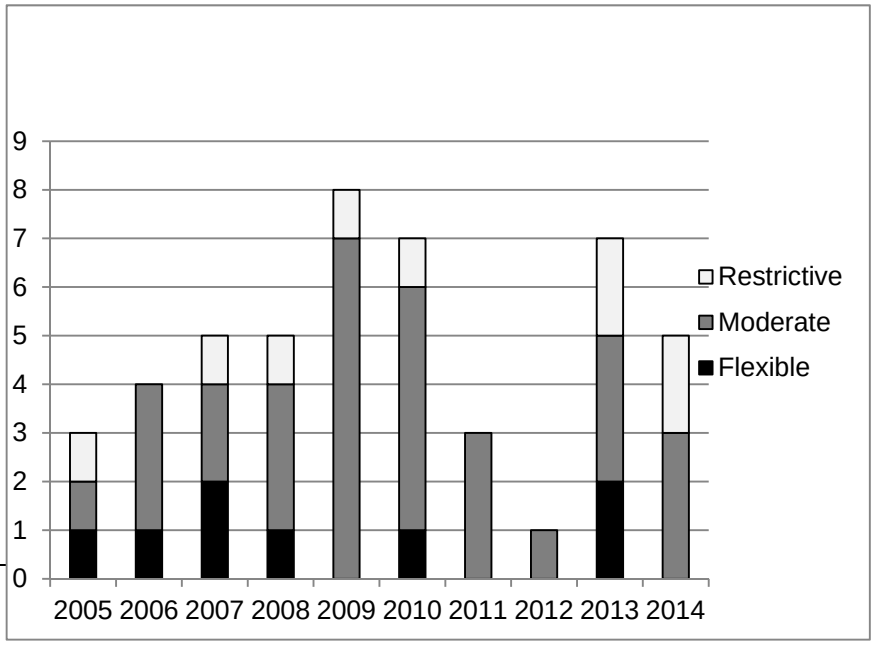


Figure 3: Data Breach Notification Information Classification[162]

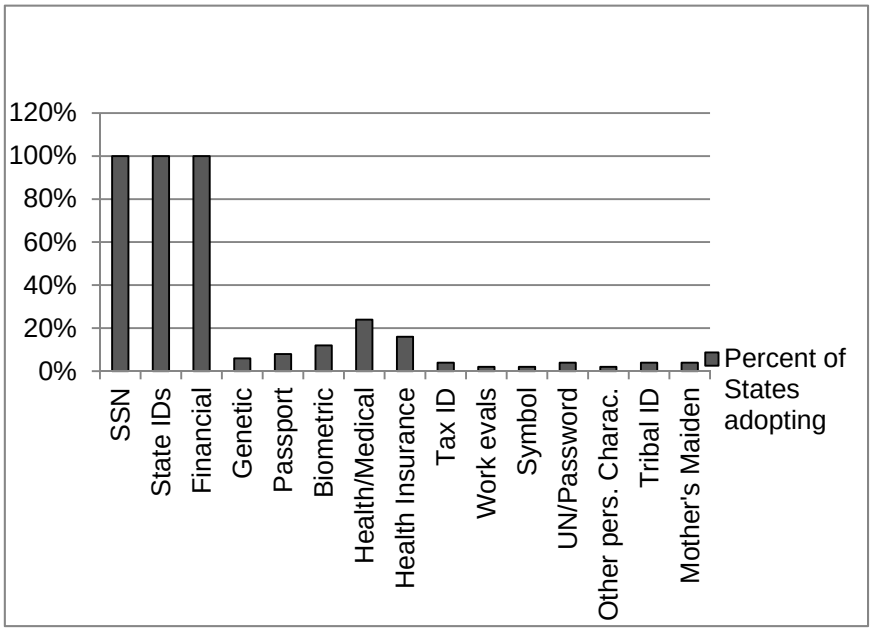
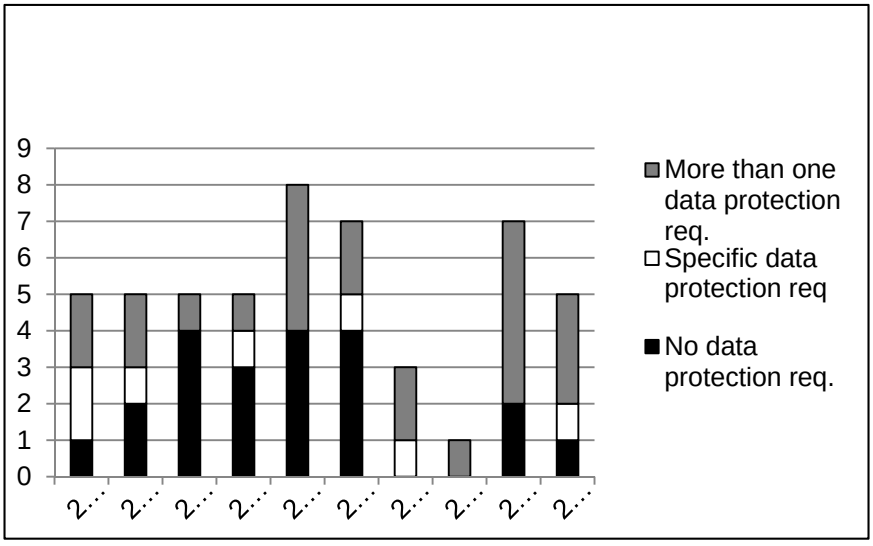
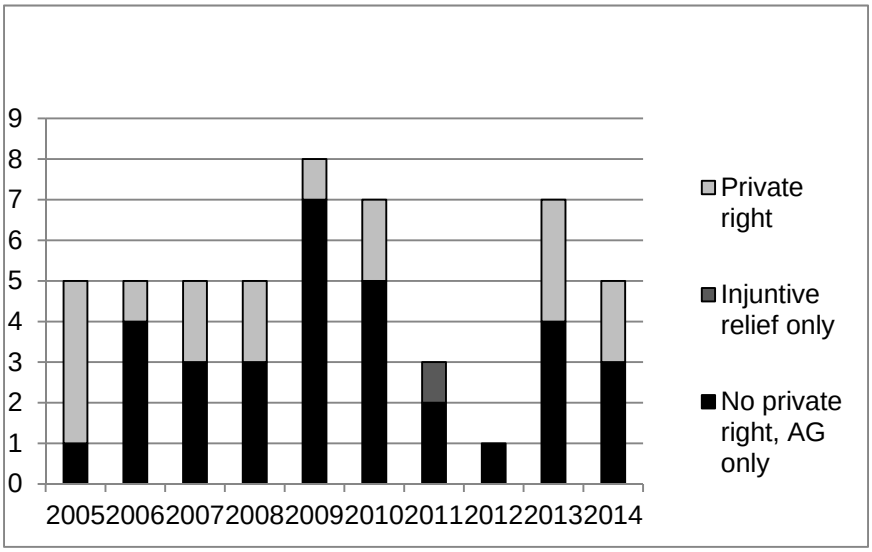



Figure 4: Data Protection Requirements by Year of Passage[163]




162. *See* statutes cited *supra* note 91.
163. *See* statutes cited *supra* note 91.

Figure 5: Private Civil Rights by Year of Passage[164]




164. *See* statutes cited *supra* note 91.