University of Colorado Law Review

Volume 87 | Issue 2 Article 7

Spring 2016

All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy

Michael D. Simpson

ALL YOUR DATA ARE BELONG TO US*: CONSUMER DATA BREACH RIGHTS AND REMEDIES IN AN ELECTRONIC EXCHANGE ECONOMY

MICHAEL D. SIMPSON**

Consumers navigating the United States' modern electronic exchange economy are uniquely vulnerable to injury from data breaches. Hackers run data breach operations on an industrial scale, with a worldwide underground economy supporting the processing and exploitation of stolen information. Economic damages from data breaches exceed millions of dollars annually in direct and indirect costs for consumers and businesses alike. While existing common law, statutory law, and regulatory law offer consumers affected by a data breach some degree of protection, that protection is largely inadequate in the face of the threat posed by consumer data breaches. This Comment argues that consumers can be better protected from the harm caused by data breaches by importing principles from European data privacy law into American law.

---

* *See All Your Base Are Belong to Us*, KNOW YOUR MEME, http://knowyourmeme.com/memes/all-your-base-are-belong-to-us [https://perma.cc/QN4J-VURL].

** J.D. Candidate, University of Colorado Law School, 2016. I am grateful to all of the members of the *University of Colorado Law Review* for their assistance during the production of this Comment. In particular, I would like to thank Mike Bohan, Larry Myers, and Ann Stanton for their insightfulness and dedication throughout the editing process; I can truly say that this Comment is better for your efforts. Most of all, I wish to thank my wife Kristen; my children Amaia, Jacob, and Maren; and my parents Doug and Carol: without all of your love and support, I would never have gotten this far. Kristen, te quiero para siempre.

INTRODUCTION

By all indications, the 2013 holiday shopping season was a disappointment for American retailers.[1] In October 2013, the National Federation of Retailers had forecast only modest sales gains over the previous year, mostly because of weak demand and low shopper confidence.[2] While retailers slashed prices for Black Friday, promoted online deal blitzes, and provided free shipping, even those modest forecasts turned out to overestimate final retail sales numbers for the season.[3] Target

1. Joshua Brustein, *Holiday Retail Sales for 2013 Are Weaker Than They Look*, BLOOMBERG (Dec. 26, 2013), http://www.bloomberg.com/bw/articles/2013-12-26/2013-holiday-sales-numbers-are-weaker-than-they-appear [http://perma.cc/ED D6-NYSX].

2. Kathy Grannis Allen, *NRF Forecasts Marginal Sales Gains This Holiday Season*, NAT'L RETAIL FED'N (Oct. 2, 2013), https://nrf.com/media/press-releases/nrf-forecasts-marginal-sales-gains-this-holiday-season [https://perma.cc/ NWU8-X58H].

3. Tiffany Hsu, *November Retail Sales Weak Despite All-Out Black Friday Efforts*, L.A. TIMES (Dec. 5, 2013), http://articles.latimes.com/2013/dec/05/ business/la-fi-mo-thanksgiving-black-friday-november-retail-sales-20131205 [http://perma.cc/CY83-82HX].

Corporation was one retailer that initially appeared to over-perform otherwise lackluster industry estimates.[4] Unfortunately, when millions of consumers exited Target stores on Black Friday, they left behind more than just their money: they also left sensitive payment card and consumer information that was quietly being exfiltrated to Russia.[5]

First publicized by a security blogger on December 13, 2013, and confirmed six days later by Target, the data breach was enormous by any standard.[6] Between November 27th and December 15th, hackers[7] stole 40 million credit and debit card numbers and 70 million other consumer records.[8] The breach cost banks and credit unions more than $200 million in card replacement costs, and Target later pledged to spend $100 million in order to upgrade outdated, unsecure payment terminals.[9]

The still-unidentified hacker or hacker group who broke into Target's network enjoyed a lucrative payday.[10] Between

---

4. *Target Announces Strong Start to Black Friday Sale with Target.com Traffic Exceeding Previous Records*, TARGET CORP. (Nov. 29, 2013), http://pressroom.target.com/news/target-announces-strong-start-to-black-friday-sale-with-target-com-traffic-exceeding-previous-records [http://perma.cc/5Y95-4K96].

5. Marie-Louise Gumuchian & David Goldman, *Security Firm Traces Target Malware to Russia*, CNN (Jan. 21, 2014, 5:50 AM), http://www.cnn.com/2014/01/20/us/money-target-breach [http://perma.cc/M7MA-EEXU].

6. Brian Krebs, *Sources: Target Investigating Data Breach*, KREBSONSECURITY (Dec. 18, 2013), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ [http://perma.cc/MDC9-QS4R].

7. As used in this Comment, a "hacker" is a person committed to unauthorized penetration of computer networks via circumvention of security measures for malicious or criminal purposes. *See, e.g.*, *Hacker (Term)*, WIKIPEDIA, https://en.wikipedia.org/wiki/Hacker_(term)#Hacker_definition_controversy [https://perma.cc/8Q8T-BXG2]. While this colloquial usage of the term is commonplace, "hacker" can actually refer to any one of several distinct and often overlapping computer subcultures, many of which are not involved in any sort of computer crime. *See id.*

8. Brian Krebs, *The Target Breach, by the Numbers*, KREBSONSECURITY (May 6, 2014) [hereinafter *Target Numbers*], http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/ [http://perma.cc/VQR2-VULW]. Other consumer records stolen included names, addresses, email addresses, and phone numbers of Target shoppers. *Id.*

9. *Id.*

10. *See* Brian Krebs, *Who's Selling Credit Cards from Target?*, KREBSONSECURITY (Dec. 24, 2013), http://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target/ [http://perma.cc/N38F-RKBP]. Using some remarkable Internet sleuthing, Krebs traced sales of the stolen Target cards to an individual named Andrew Hodirevski who lives or lived in Odessa, Ukraine. *Id.* Although Krebs could not definitively conclude that Hodirevski was involved in the actual hacking of Target, he considers it a good bet that Hodirevski at least

one and three million of the cards stolen from Target were later successfully sold on the black market and used fraudulently.[11] The first batch of purloined cards sold for as much as $44.80 apiece in the days leading up to Target's public acknowledgement of the breach on December 19, 2013.[12] After the announcement, prices dropped precipitously to as little as $8.00 each.[13] Estimated by the median price of $26.85 per card, hackers could have generated as much as $53.7 million in revenue from the breach.[14]

The breach had an immediate impact on Target's earnings and executive management. Profits dropped 46% in the fourth quarter of 2013 compared to the previous year, mostly due to reduced sales and costs associated with responding to the breach.[15] Target's stock price dropped 11% between December 19, 2013, and February 26, 2014.[16] The breach was the last straw on the back of the already troubled tenure of Target's CEO, leading the Board of Directors to ask for his resignation in May 2014.[17] Unsurprisingly, litigation followed soon after the breach was confirmed.[18] Seventy-six separate federal class

---

knows who amongst the Russian criminal underground *was* involved. *Id.*

11. *Target Numbers*, *supra* note 8.

12. Brian Krebs, *Fire Sale on Cards Stolen in Target Breach*, KREBSONSECURITY (Feb. 19, 2014), http://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach/ [http://perma.cc/29QJ-T4LQ].

13. *Id.* Generally, batches of stolen cards are bundled into "bases," or tranches, and released for sale at the same time on underground card shops. Stolen cards from a base released before Target's breach acknowledgement sold for between $26.60 and $44.80 each, while stolen cards from a base released two months after Target's acknowledgment sold for between $8.00 and $28.00, a drop in price of as much as 70%. The price drop appears to have been due to the declining "valid rate," or the percentage of cards in a given base that could be expected to work. The pre-acknowledgement base was advertised as 100% valid, while the later base only had a 60% valid rate. Valid rates are expected to decline after a data breach is disclosed and card issuers begin to cancel stolen cards. *Id.*

14. *Target Numbers*, *supra* note 8. Krebs used the midpoint of the stolen card sales range estimate for his calculation. *Id.* Accordingly, the figure could be off by as much as 50% either way.

15. *Target Numbers*, *supra* note 8.

16. Andria Cheng, *Two Months After Damaging Data Breach, Target Stock Has Its Best Day in 5 Years*, MARKETWATCH: BEHIND THE STOREFRONT (Feb. 26, 2014, 2:11 PM), http://blogs.marketwatch.com/behindthestorefront/2014/02/26/two-months-after-damaging-data-breach-target-stock-has-its-best-day-in-5-years [http://perma.cc/9WNU-5GDQ].

17. Elizabeth A. Harris, *Faltering Target Parts Ways with Chief*, N.Y. TIMES (May 5, 2014), http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html [http://perma.cc/R92P-T35P].

18. Kyla Asbury, *Target Data Breach Class Actions Form MDL Proceeding in Minnesota*, LEGAL NEWSLINE (Apr. 25, 2014, 7:13 PM), http://legalnewsline.com/

actions (divided into financial institution cases, consumer cases, and shareholder cases) were consolidated into one action in the United States District Court for the District of Minnesota.[19] The Target plaintiffs alleged a number of causes of action, including negligence, breach of contract, and violations of state breach notification laws.[20] Unfortunately for the plaintiffs, the state of consumer data breach law means that their case will be difficult, if not impossible, to make.

This Comment argues that, under current law, consumer rights and remedies are inadequate in the event of a data breach. Further, it argues that consumers can be protected from the harm caused by data breaches by importing principles from European data privacy law. Part I lays a foundation for understanding the context of data breaches in our modern electronic exchange economy. Part II reviews and analyzes the current state of consumer rights and remedies under common law, statutory law, and regulatory law. Finally, Part III discusses a proposal for enhancing consumer rights and remedies by importing principles from European data privacy law.

I. BACKGROUND

Cash is no longer king for modern American consumers. In 2011, 66% of in-person point-of-sale transactions[21] used plastic cards of one kind or another, including credit cards, debit cards, prepaid credit cards, and gift cards.[22] Cash is expected to comprise only 23% of point-of-sale transactions by 2017.[23] Accounting for a mere 7% of transactions,[24] paper checks are

issues/class-action/248819-target-data-breach-class-actions-form-mdl-proceeding-in-minnesota [http://perma.cc/YSC7-3UTC].

19. *In re* Target Corporation Customer Data Security Breach Litigation, No. 14-MD-02522 (D. Minn. Apr. 14, 2014), 2014 WL 10355867.

20. *See generally* Consumer Plaintiffs' Consolidated Class Action Complaint, *In re* Target Corporation Customer Data Security Breach Litigation, No. 14-MD-02522 (D. Minn. Aug. 25, 2014), 2014 WL 4954585.

21. A point-of-sale transaction occurs when a consumer makes a payment to a merchant in exchange for goods or services. *Point of Sale*, WIKIPEDIA, https://en.wikipedia.org/wiki/Point_of_sale [https://perma.cc/ZG6B-RYDT].

22. Catherine New, *Cash Dying as Credit Card Payments Predicted to Grow in Volume: Report*, HUFFINGTON POST (June 7, 2015, 12:07 PM) http://www.huffingtonpost.com/2012/06/07/credit-card-payments-growth_n_1575417.html [http://perma.cc/BDA8-LDFC].

23. *Id.*

24. *Id.*

even more endangered than cash, and the Federal Reserve estimates that check use could disappear entirely by 2026.[25] Our economy largely runs on an electronic exchange, and the switch to an electronic exchange economy has exponentially multiplied the security risks to the average consumer.

Cash, of course, is completely anonymous. However, credit and debit cards by their very nature cannot be. The magnetic strip on the back of a credit card contains all the information necessary to verify a transaction: bank name, primary account number, cardholder's name, expiration date, and more.[26] After a card is swiped at a retailer's point-of-sale system the necessary transaction and card information is sent to a store server, then to the merchant's main computer system, then to the card processor, then to the bank, and then all the way back up the line again to the store.[27] All told, a transaction is approved or declined in around .06 seconds.[28]

As anyone who has ever waited in line behind someone slowly writing a check can attest, the speed and convenience of credit cards makes point-of-sale transactions quick and easy for consumers and retailers alike. However, that speed and convenience comes at a steep price in security. At its root, our current verification system relies on forty-year-old technology to authenticate card numbers.[29] Magnetic strip credit cards first entered common use in the 1970s,[30] and they worked just fine until the 1990s when personal computers made card

25. David B. Humphrey & Robert Hunt, *Getting Rid of Paper: Savings from Check 21*, at 17 (Research Dep't, Fed. Reserve Bank of Phila., Working Paper No. 12-12, 2012).

26. J.D. Biersdorfer, *Q & A: A Wealth of Information Inside a Magnetic Strip*, N.Y. TIMES (Jan. 17, 2002), http://www.nytimes.com/2002/01/17/technology/q-a-a-wealth-of-information-inside-a-magnetic-strip.html [http://perma.cc/V42B-MV6M].

27. Charles Lane, *The Holidays Bring a New Season for Credit Card Breaches*, NPR (Oct. 12, 2014, 12:26 PM), http://www.npr.org/2014/10/12/355511381/the-holidays-bring-a-new-season-for-credit-card-breaches [http://perma.cc/QJ85-7PCX].

28. *Id.*

29. *Id.*

30. Damien Gayle, *The World's First Magnetic Stripe Credit Card Up for Sale: Relic of Financial History to Go Under the Hammer at Sotheby's New York*, DAILY MAIL (Dec. 4, 2012), http://www.dailymail.co.uk/sciencetech/article-2242897/Worlds-magnetic-strip-credit-card-hammer-Sothebys-New-York.html [http://perma.cc/PPB7-9TUB]. IBM developed magnetic strip cards in the late 1960's. *Id.* In 1970, American Express became the first card issuer to adopt the new technology. *Id.*

counterfeiting easy.[31] With no way to quickly verify the authenticity of a given card, merchants could easily be defrauded by anyone with a computer and a stack of card blanks.[32]

Thanks to the strong telecom network in the United States, American retailers started using online systems to verify credit card authenticity.[33] Online systems, usually using a modem-equipped terminal, send transaction information (including 16-digit card numbers) across telephone lines in text form to third-party payment processors.[34] The processor, in turn, contacts the card issuer, who then approves (or declines) the transaction according to the funds available in the consumer's account.[35] The payment processing industry itself is bewilderingly vast, with thousands of companies offering services.[36]

Unfortunately, retailers and banks have been loath to update 20th century authentication systems with 21st century security technologies.[37] Used for many years in Europe and elsewhere around the world, so-called "chip-and-PIN" cards encrypt and store card data on an embedded microchip, which is much harder to duplicate than a standard magnetic strip.[38] They also require a Personal Identification Number (PIN) to work.[39] Because a transaction requires both the card and a PIN, it works as a much more secure two-factor authentication procedure, forcing thieves to have both pieces of information to

31. Lane, *supra* note 27.

32. *See id.*

33. *Id.*

34. Odysseas Papadimitriou, *How Credit Card Transaction Processing Works: Steps, Fees, and Participants*, CARDHUB (Apr. 2, 2009), http://www.cardhub.com/edu/credit-card-transaction/ [http://perma.cc/YAE7-VWYV].

35. *Id.*

36. For example, Visa International, Inc., lists over 3,600 payment processors in its global registry. *Visa Global Registry of Service Providers*, VISA, http://www.visa.com/splisting/searchGrsp.do [http://perma.cc/YH5K-DUT7] (last updated Aug. 28, 2015).

37. *See* David Dayen, *Your Credit Card Has a Dangerous Flaw That the Banks Refuse to Fix*, NEW REPUBLIC (Jan. 16, 2014), http://www.newrepublic.com/article/116236/credit-card-magnetic-stripes-are-putting-you-risk-identity-theft [http://perma.cc/ZG3W-YYJV].

38. Susan Johnston, *Coming Next Fall: More Chip and PIN Cards in the U.S.*, U.S. NEWS & WORLD REP. (Oct. 28, 2014, 9:21 AM), http://money.usnews.com/money/personal-finance/articles/2014/10/28/coming-next-fall-more-chip-and-pin-cards-in-the-us [http://perma.cc/GK7P-622L].

39. *Id.*

use the card successfully.[40] Newer formats like "Europay, MasterCard, Visa," or "EMV," promise to produce credit cards even more secure than the older chip-and-PIN versions.[41] Even so, chip-and-PIN and EMV cards still store account information physically, leaving it vulnerable to hackers.[42] Newer payment systems such as Google Wallet and Apple Pay use a system called tokenization, which replaces a credit card number with a randomly generated, one-time use number for transmission during authentication, thus protecting the cardholder's account information.[43]

The significant system upgrades required for both retailers and banks to use new card technologies has led to a chicken-and-egg problem with adaptation in the United States.[44] Retailers need new card readers to handle more secure cards, but do not want to spend the money until they know banks will issue them.[45] Banks, in turn, do not want to issue more expensive, secure cards until retailers install new card readers.[46] With neither side willing to spend money before the other, card authentication in the US has been stuck in a technological purgatory for most of the past decade. Ultimately, payment processors plan to force the issue by assigning liability for payment fraud to banks who refuse to issue chip-and-PIN cards, thus giving at least one side a significant financial interest in spending the money necessary to update US authentication systems.[47]

Outdated transaction technologies are largely to blame for turning the US economy into a fertile field for hackers.[48] To

40. Dayen, *supra* note 37.

41. Robert Harrow, *Credit Card Fraud: Why EMV Matters in the U.S.*, HUFFINGTON POST (Aug. 5, 2015, 9:10 AM), http://www.huffingtonpost.com/robert-harrow/credit-card-fraud-why-emv_b_7929310.html [http://perma.cc/K995-L9VH].

42. Dayen, *supra* note 37

43. Lane, *supra* note 27.

44. Dayen, *supra* note 37.

45. *Id.*

46. *Id.*

47. Tom Risen, *Credit Cards Will Get Security Upgrade in 2015*, U.S. NEWS & WORLD REP. (Feb. 11, 2014, 3:24 PM), http://www.usnews.com/news/articles/2014/02/11/credit-cards-will-get-security-upgrade-in-2015 [http://perma.cc/4FEZ-MFUJ]. Visa and MasterCard required US merchants to make the transition by October 2015 in order to avoid liability. *Id.*

48. *See* Ross Kerber, *Target Payment Card Data Theft Highlights Lagging U.S. Security*, REUTERS (Dec. 22, 2013, 9:00 AM), http://www.reuters.com/article/2013/12/22/target-security-lagging-idUSL2N0K004A20131222 [http://

understand just how fertile, it is helpful to know how data breaches work, what happens to the data stolen in a breach, and how much breaches cost companies and consumers.

A. Anatomy of a Data Breach

Data breaches can happen in a multitude of ways.[49] Investigation into the root causes of data breaches has revealed three main types of breaches: well-meaning insiders, targeted attacks, and malicious insiders.[50] Many breaches are a combination of two or more of these breach types.[51] For example, targeted attacks are often made possible by well-meaning employees who fail to comply with security policies, thus leading to a breach.[52] Regardless of the source, almost all breaches share four characteristic phases: incursion, discovery, capture, and exfiltration.[53]

During the incursion phase, hackers break into a company network by exploiting system vulnerabilities, such as password policy violations,[54] targeted malicious software,[55] or SQL injections.[56] After gaining access to the network, hackers

---

perma.cc/Y9LX-4ZD8]. Nearly half of worldwide card fraud losses in 2012 occurred in the US.

49. *See, e.g.*, VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT (2014). Verizon tracks ten general categories of data breaches, including Point-of-Sale Intrusions, Malware, and Insider and Privilege Misuse. *Id.*

50. SYMANTEC, ANATOMY OF A DATA BREACH: WHY BREACHES HAPPEN AND WHAT TO DO ABOUT IT 2 (2009).

51. *Id.*

52. *Id.*

53. *Id.* at 4.

54. Password policy violations refer generally to any violation of an organization's computer password policy. *See Password Standard*, U. GA. ENTERPRISE INFORMATION TECH. SERVS., http://eits.uga.edu/access_and_security/infosec/pols_regs/policies/passwords/password_standard/ [http://perma.cc/94B4-CZ9T]. Violations can be mechanical (creating weak passwords, or passwords without required characteristics) or social (sharing passwords, writing passwords down, or sending unencrypted passwords via email). *Id.* For an example of a very detailed password policy, including construction guidelines and violation consequences, *see id.*

55. Malicious code describes any software code or script intended to cause a security breach or damage to a computer system, and includes a broad array of software such as viruses, worms, Trojan horses, and backdoors. *See, e.g.*, *What Is Malicious Code?*, KASPERSKY LABS, https://usa.kaspersky.com/internet-security-center/definitions/malicious-code#.VZ3-lflViko [https://perma.cc/HY3D-N6U7]. Targeted malicious code is software carefully tailored and designed to attack a specific computer or computer network. *Id.*

56. SQL injection is a hacking technique in which malicious SQL ("Structured

discover sensitive data by scanning the network and mapping out the company's systems.[57] Once confidential data is found, hackers capture it either directly from unprotected systems, or by installing surreptitious components on targeted servers and network access points, capturing sensitive data as it flows through the company's network.[58] Finally, the confidential data is exfiltrated from the compromised network and sent back to the hackers.[59]

Studies of the Target data breach show that it appears to have been a classic multiple factor failure case. Sometime before the breach, Target gave network access to a small Pennsylvania HVAC vendor with poor security practices.[60] The hackers seem to have found the vendor using simple Internet searches which, at the time, showed Target's supplier portal and facilities management page.[61] At least two months before the breach, the hackers sent malware-laden emails to the vendor and acquired the vendor's Target login information.[62] They then leveraged the vendor's access to break into poorly secured portions of Target's network, and from there were able to access the most sensitive areas of the network.[63] Subsequently, it was fairly simple for the hackers to discover, collect, and exfiltrate tens of millions of confidential records.[64]

Despite what might be expected from the Target breach,

Query Language," a very common database programming language) instructions are inserted into a compromised program for execution. SQL injections exploit security vulnerabilities in application software to run commands advantageous to a hacker's goals. *See, e.g.*, *SQL Injection*, WIKIPEDIA, http://en.wikipedia.org/wiki/SQL_injection [http://perma.cc/H7ZS-4C4Z].

57. ANATOMY OF A DATA BREACH, *supra* note 50, at 4.

58. *Id.*

59. *Id.*

60. SENATE COMM. ON COMMERCE, SCI., AND TRANSP., 113TH CONG., A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH 4 (2014), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883 [http://perma.cc/M8RS-WUQU].

61. *Id.* at 7.

62. *Id.* at 8. The vendor most likely fell victim to a "phishing" attack, a well-known method in which an attacker uses social engineering techniques to trick unwary recipients into accepting official-looking emails which direct them to click a link, log in, and verify their information; the link actually directs the user to computers controlled by the attacker, thus allowing the attacker to collect the user's login credentials. *Phishing*, WIKIPEDIA, https://en.wikipedia.org/wiki/Phishing [https://perma.cc/T7DN-9U6E].

63. *Id.* at 8–9.

64. *Id.* at 8–10. Once the attack was established on Target's network, the company appears to have ignored multiple alerts that could have broken the "kill chain" before the breach was severe. *Id.*.

most hackers do not seem to be motivated solely by financial gain.[65] Fully fifty-one percent of hackers surveyed by the software firm Thycotic were motivated by "thrill-seeking" and were "simply curious, bored, or want[ed] to test out their abilities."[66] This may explain why the confidential information taken in high-profile data breaches is often sold off wholesale at a discount to illicit overseas data brokers instead of used directly by the person who hacked it.[67] Once out of the country and released onto the black market, stolen data enters an economic ecosystem just as sophisticated as the market supporting any legitimate commodity.[68]

B. Industrial Data Theft

Data theft works much like any legitimate supply chain. "First come the manufacturers, then the wholesalers, the middlemen, the retailers and, finally, consumers."[69] Hackers are manufacturers who steal huge numbers of credit cards via a data breach.[70] In the past, the raw card numbers might have been used for expensive online purchases, but card issuers now employ sophisticated anti-fraud algorithms that quickly detect anomalous transactions on compromised accounts.[71] Now, the numbers go to wholesalers overseas who break them down into manageable groups of cards sorted by geographic area and ZIP code.[72]

Wholesalers offer up the bundles for sale in bulk on

65. THYCOTIC, THYCOTIC BLACK HAT 2014 HACKER SURVEY EXECUTIVE REPORT 2 (2014). Only eighteen percent of "black hat" hackers (a hacker who violates computer security for malicious or illegal reasons) surveyed by software firm Thycotic reported being motivated by financial gain. *Id.* Note that the survey respondents were self-identified hackers attending the Black Hat USA 2014 security conference, *id.*, so results may be biased in favor of non-financially motivated individuals.

66. *Id.*

67. *See* Elizabeth Weise, *Massive Data Breaches: Where They Lead Is Surprising*, USA TODAY (Oct. 3, 2014), http://www.usatoday.com/story/tech/2014/10/02/home-depot-data-breach-credit-card-fast-food/16435337/ [http://perma.cc/J9ZC-E7JM].

68. *See* Wade Williamson, *The Underground Economy of Data Breaches*, FORBES (June 18, 2014) [hereinafter *Underground Economy*], http://www.forbes.com/sites/frontline/2014/06/18/the-underground-economy-of-data-breaches/ [http://perma.cc/VG2F-9VPL].

69. Weise, *supra* note 67.

70. *Id.*

71. *Id.*

72. *Id.*

underground websites, often with money-back quality guarantees.[73] Middlemen buy up the bundles and generate cloned credit cards using readily available machines and blank cards.[74] Newly cloned cards are then sold to low-level criminals or gangs who retail them on the street or launder them by purchasing difficult-to-trace gift cards.[75]

Customers who purchase cloned cards generally do not use them for high-dollar transactions.[76] One credit union affected by the September 2014 Home Depot data breach saw average fraud of only $201 on fake cards.[77] End users of stolen credit cards are often low-income people charging small amounts at McDonalds or Walmart for a week or so, until the credit card issuer cancels the card.[78] Essentially, hackers insulate themselves from risk by processing the raw numbers they steal through so many hands that law enforcement has almost no one left to target.[79] Even if players in the chain can be prosecuted, the detailed investigations required can last for years and face uncertain multinational cooperation.[80] For

73. *Id.*

74. *See* Wade Williamson, *What Happens to Stolen Data After a Breach?*, SECURITYWEEK (Mar. 17, 2014), http://www.securityweek.com/what-happens-stolen-data-after-breach [http://perma.cc/9XLV-STMZ]. A carding operation can cost around $500 online. Weise, *supra* note 67.

75. *Underground Economy*, *supra* note 68. Retailer branded gift cards are difficult to trace because, once purchased, they are essentially the same as cash, although they can only be used at a specific retailer. *Id.* Prepaid credit cards are especially problematic because they are not tied to a specific bank account, can be reloaded remotely, are accepted almost anywhere, and can be used anonymously. Frank Bajak, *Prepaid Credit Cards Being Used to Launder Money Across the Border*, HUFFINGTON POST (May 23, 2011), http://www.huffingtonpost.com/2011/05/23/prepaid-cards-being-used-to-launder_n_865464.html [http://perma.cc/ZM77-VTD5]. Prepaid credit cards are increasingly used by drug cartels for money laundering because they can easily transport tens of thousands of dollars per card across United States borders without triggering the $10,000 cash declaration requirement. *Id.*

76. Weise, *supra* note 67.

77. *Id.*

78. *Id.*

79. *See id.*

80. *See, e.g.*, Samantha Henry, *Largest Hacking, Data Breach Prosecution in U.S. History Launches with Five Arrests*, SAN JOSE MERCURY-NEWS (July 25, 2013), http://www.mercurynews.com/business/ci_23730361/largest-hacking-data-breach-prosecution-u-s-history [http://perma.cc/8EB5-NHX9]. Launched after a 2007 data breach involving the theft of over 160 million card numbers from several companies, this investigation took nearly five years to yield a 2013 indictment naming four Russians and one Ukrainian. *Id.* Only one defendant was in US custody at the time of the indictment, with another awaiting extradition from the Netherlands. *Id.* The other three defendants remained at large, most

affected consumers, law enforcement efforts[81] have little, if any, bearing on remedying their personal damages.

C. Economic Costs of Data Breaches

The threat of data breaches is growing just as our electronic economy is growing. The Privacy Rights Clearinghouse (PRC), a California non-profit dedicated to protecting the privacy of American consumers,[82] estimates that there have been over 4,600 publicly reported data breaches involving nearly one trillion records in the United States since 2005.[83] Because a single consumer may have multiple records stolen in any given breach, it may be impossible to calculate the total number of individual consumers affected.[84] PRC's numbers only include breaches reported by the breached entity to affected customers or to a government agency.[85] The actual

---

likely in Russia. *Id.*

81. Because this Comment focuses on consumer rights and remedies for data breaches, rather than data breaches in a criminal context, law enforcement efforts to combat cybercrime are beyond the scope of this discussion. However, the reader should be aware that numerous state and federal agencies dedicate considerable resources to fighting cybercrime generally. *See, e.g.*, FED. BUREAU OF INVESTIGATION, *Cyber Crime*, https://www.fbi.gov/about-us/investigate/cyber [https://perma.cc/2L9Z-AYKR] (detailing FBI cybercrime investigation priorities); DEP'T OF HOMELAND SEC., *Combating Cyber Crime*, http://www.dhs.gov/topic/combating-cyber-crime [http://perma.cc/H4BC-JG8P] (discussing cybercrime efforts of DHS components such as the US Secret Service and US Immigration and Customs Enforcement); COLO. BUREAU OF INVESTIGATION, *Identify Theft/Cyber Crimes Unit Role*, https://www.colorado.gov/pacific/cbi/identity-theftfraud-and-cyber-crimes-unit-role [https://perma.cc/87KE-DLRV] (describing the Colorado Bureau of Investigation's role in investigating identity theft, fraud, and cybercrime).

82. *About the Privacy Rights Clearinghouse*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/content/about-privacy-rights-clearinghouse [https://perma.cc/38RQ-M7LJ].

83. *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breach [https://perma.cc/9JJD-94SA].

84. *Chronology of Data Breaches: FAQ – What Does the Total Number Indicate?*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breach-FAQ#1 [https://perma.cc/8JTH-H5NB]. PRC's numbers include records such as Social Security numbers, credit card account numbers, and driver's license numbers. *Id.* A single consumer could have multiple different records stolen in a single breach, or separate individual records stolen in multiple different breaches. *Chronology of Data Breaches: FAQ – What Does the Chronology of Data Breaches Contain?*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breach-FAQ#1 [https://perma.cc/8JTH-H5NB].

85. *Chronology of Data Breaches: FAQ – Is the Chronology of Data Breaches a Complete Listing of All Breaches?*, PRIVACY RTS. CLEARINGHOUSE,

numbers are likely far greater. One recent survey found that 57% of analysts working on enterprise-related breaches for US companies have countered security intrusions that were not publicly disclosed.[86] The numbers increased to 66% of analysts working for companies with more than 500 employees.[87] Considering that one report found 621 confirmed data breaches in 2012, and that two-thirds of analysts admitted to working on undisclosed breaches, the number of attacks in 2012 (the most recent year with data available) may have been significantly underreported.[88] There is little reason to believe that underreporting rates have improved since 2012.[89]

The financial costs of a data breach, however, are very clear. In 2014, the average cost of a data breach to an organization was $5.9 million, or $201 per breached record.[90] In addition to direct costs, a breach can cost $3.2 million in lost business, as well as $1.6 million in post-breach response costs, such as activities addressing victim and regulator concerns, legal and consulting fees, and identity protection services.[91] Indirect costs are far more difficult to assess than direct costs, but one recent survey found that 54% of all American consumers, not just those affected by a breach, "would never, or were very unlikely to, shop or do business again with a company that had experienced a data breach where financial data was stolen."[92] Of course, the survey responses have not been borne out in actual behavior, with consumers now appearing much less likely to financially penalize a breached

---

https://www.privacyrights.org/data-breach-FAQ#1 [https://perma.cc/8JTH-H5NB].

86. Charlie Osborne, *Enterprise Data Breaches Often Left Undisclosed, Malware Analysts Say*, ZERO DAY (Nov. 11, 2013), http://www.zdnet.com/enterprise-data-breaches-often-left-undisclosed-malware-analysts-say-7000023032/ [http://perma.cc/959Q-QZEP].

87. *Id.*

88. *Id.*

89. *See, e.g.*, Don Jergler, *Secret Service Agent Says Many Cyber Breaches Go Unreported*, INS. J. (Mar. 7, 2014), http://www.insurancejournal.com/news/west/2014/03/07/322748.htm [http://perma.cc/MCD9-UX2P].

90. PONEMON INST., 2014 COST OF DATA BREACH STUDY: UNITED STATES 1 (May 2014).

91. *Id.* at 2–3.

92. *Global Survey Reveals Impact of Data Breaches on Customer Loyalty*, SAFENET, INC. (Jul. 30, 2014), http://www.safenet-inc.com/news/2014/data-breaches-impact-on-customer-loyalty-survey/ [http://perma.cc/JR4J-UUPV]. Despite the numbers, Americans appear to be much more likely to continue patronizing a breached establishment than our foreign counterparts are: 68% of British, 72% of Australian, and 82% of Japanese consumers would not do business again with a company that experienced a data breach. *Id.*

company than in years past.[93]

Aside from retailers, banks and other financial institutions are among the first to bear the initial costs of data breaches. The cost to banks affected by the Target data breach alone has exceeded $240 million.[94] That figure only represents direct card replacement costs for compromised accounts and does not factor in fraudulent activity on those accounts.[95] Although replacement costs do not come directly out of consumers' pockets,[96] Target is not yet liable for the expenses either, pending the outcome of the Target data breach litigation. Even if banks are successful in their litigation, they will likely only be able to recover the cost of any fraud associated with stolen cards, not card replacement costs.[97] Financial institutions are essentially forced to absorb the costs retail data breaches impose on them.[98] However, banks can eventually recover at least some of their expenses by passing those costs on to their customers through higher credit card interest rates and assorted bank fees.[99] As often seems to be the case when dealing with data breaches, consumers will ultimately pay in one form or another.[100]

---

93. Sarah Halzack, *Home Depot and JP Morgan Are Doing Fine. Is It a Sign We're Numb to Data Breaches?*, WASH. POST (Oct. 6, 2014), http://www.washington post.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/ [http://perma.cc/Y6MR-R8RD]. According to the article, consumers may be experiencing "data breach fatigue" due to the sheer number of high-profile breaches occurring in the past few years. *Id.* Consumers may also feel that data breaches are "unavoidable," and that they have no choice about where to shop for certain goods. *Id.*

94. Christine DiGangi, *The Target Data Breach Has Cost Banks $240 Million . . . So Far*, CREDIT.COM (Feb. 21, 2014), http://blog.credit.com/2014/02/target-data-breach-cost-banks-240-million-76636 [http://perma.cc/G6H3-TJ8C]. This figure was reported by member institutions of the Consumer Banker Association, the Credit Union National Association, and the Independent Community Bankers Association. *Id.* Actual costs would be much greater if the impact of fraudulent activity and card replacement costs to banks not members of these associations is factored in. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

98. *See* Ryan Tracy, *In a Cyber Breach, Who Pays, Banks or Retailers?*, WALL STREET J. (Jan. 12, 2014), http://www.wsj.com/articles/SB10001424052702303819704579316861842957106 [http://perma.cc/E535-2KHF].

99. J. Craig Anderson, *Data Breaches Troubling Banks More Than Consumers*, PORTLAND PRESS HERALD (Sept. 6, 2014), http://www.pressherald.com/2014/09/06/data-breach-pains-banks-more-than-consumers/ [http://perma.cc/F4Z8-R3LY].

100. *Id.*

Individual consumer costs from data breaches in general can be significant but, sometimes, difficult to reliably quantify.[101] However, a study done following a 2012 Medicaid data breach in Utah[102] estimated that each incident of fraud would result, on average, in more than $3,300 in losses to each affected consumer.[103] In addition, the study estimated that each affected consumer would be required to spend about twenty hours in time lost from work to resolve the breach, and incur approximately $770 in attorney's fees.[104]

Totaling up the worldwide costs of data breaches and other cybercrime to organizations, financial institutions, and consumers, one recent study estimated that the global economy lost more than $400 billion dollars in 2013 alone.[105] Another recent study projected that global economic losses from data breaches and cybercrime will reach two trillion dollars by 2019.[106] With such notable financial impacts on both an

101. Steve Anderson, *Quantifying the Unquantifiable: What Cost Comes with a Data Breach?*, CONTACT CENTER SOLUTIONS (Sept. 12, 2014), http://callcenterinfo.tmcnet.com/Analysis/articles/388855-quantifying-unquantifiable-what-cost-comes-with-data-breach.htm [http://perma.cc/DNM6-CQ8Z] ("When it comes to data breaches, pinning down an actual dollar value can be difficult. It's not like it would be in the case of a physical breach, where actual things would be taken and the dollar value of said items can be easily compiled and reported. In some cases, a data breach results in nothing really missing; the data that was there is still there, it's just been accessed illicitly. . . . It is also the value of cleaning up afterward, of protecting customers from potential shortfalls that said customers had no hand in, even shoring up security against future breaches later. The value of damaged reputations is also important, and that can be an even bigger loss than anything else.").

102. Kirsten Stewart, *Scope of Utah Medicaid Data Breach Explodes*, SALT LAKE TRIB. (Apr. 10, 2012), http://www.sltrib.com/sltrib/news/53879423-78/medicaid-officials-information-breach.html.csp [http://perma.cc/U3NN-CW68]. The breach exposed the Social Security numbers of 280,000 Utahns on public health insurance and less sensitive personal information of 500,000 others. *Id.* Ultimately, one in every six Utahns were directly affected by the breach. *Id.* The breach was caused by a contractor who put an unencrypted server online without proper security, and hackers were able to exfiltrate more than three-quarters of a million records in approximately one day before the breach was detected and shut down. *Id.*

103. Ann Carrns, *The Costs to Consumers of a Data Breach*, N.Y. TIMES: BUCKS (Apr. 30, 2013), http://bucks.blogs.nytimes.com//2013/04/30/the-cost-to-consumers-of-a-data-breach [http://perma.cc/8Z8K-XU7V]. It should be noted that consumer costs resulting from stolen Social Security numbers are likely to be greater than costs from stolen credit card numbers, due largely to identity theft concerns associated with Social Security numbers. *Id.*

104. *Id.*

105. CTR. FOR STRATEGIC & INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 2 (2014).

106. JUNIPER RESEARCH, CYBERCRIME AND THE INTERNET OF THREATS 5

individual and global level, consumers affected by a data breach might understandably believe that robust protections and legal remedies would be available to them. As this Comment will discuss in Part II, such consumers would be sadly disappointed in the current state of the law.

II. CONSUMER RIGHTS AND REMEDIES UNDER CURRENT LAW

For consumers affected by a data breach, understanding what rights and remedies exist for them can be difficult. As any affected consumer soon discovers, currently available rights and remedies are largely opaque, inefficient, and mostly inadequate. Under current law, consumer rights and remedies fall into three main categories: the common law of torts, statutory rights, and regulatory law. Each category will be described in the subsections that follow.

A. Common Law of Torts

Data breach plaintiffs in recent years frequently rely on common law tort claims of negligence as a cause of action. As is standard for other negligence claims, a data breach negligence claim requires that the plaintiff prove (1) the existence of a duty of care, (2) a breach of that duty, (3) causation, and (4) damages.[107] As with any other standard negligence claim, the data breach plaintiff must rely heavily on the specific facts of their case, which can be problematic in the context of a consumer data breach.[108]

For individual data breach plaintiffs, showing the elements of negligence has proven to be difficult. Most courts are reluctant to find a duty of care in data breach cases, especially when the plaintiff and defendant (as consumer and payment

(2015).

107. *E.g.*, Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010).

108. It should be noted that a consumer harmed by a data breach has no practical cause of action against a hacker for theft or other property violations: in the unlikely event that an affected consumer could actually find the hacker in order to sue him personally, the hacker would likely be judgment-proof. *See* Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers,* SCIENTIFIC AMERICAN (June 11, 2011), http://www.scientificamerican.com/article/tracking-cyber-hackers/ [https://perma.cc/AQ6N-5N32]. Thus, suing a breached entity for negligence is the logical way for a consumer to seek some sort of remedy.

processor) have no direct relationship.[109] Individual plaintiffs have also had problems overcoming difficulties associated with showing cognizable injury and causation.[110] And finally, they often struggle to defeat the economic loss rule,[111] which in most jurisdictions states that damages for purely economic losses are not recoverable based on tort theory when unaccompanied by physical property damage or personal injury.[112]

Corporate data breach plaintiffs have been somewhat more successful in pursuing their negligence claims, at least in the early stages of litigation. For example, the Fifth Circuit recently reversed a district court's dismissal of a card-issuing bank's negligence claims against a card payment processor.[113] However, some federal district courts and state courts have been unwilling to find a duty of care between card-issuing banks and breached retailers.[114] Thus, case law is currently unsettled on the validity of negligence as a theory for recovery in data breach cases. Accordingly, defendants are likely to vigorously contest the imposition of a duty of care in negligence cases. Target, for example, filed a motion to dismiss, arguing that the "Banks have failed to plead that Target owed the Banks any duty of care or that Target breached any such duty."[115] Unfortunately for Target, the district court disagreed

109. Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES: LEADING LAWYERS ON NAVIGATING CHANGES IN SECURITY PROGRAM REQUIREMENTS AND HELPING CLIENTS PREVENT BREACHES (2014), 2014 WL 10442, at *7.

110. *Id.*; *see also* Bell, et al. v. Blizzard Entertainment, Inc., No. 12-CV-09475, at 11, 14 (C.D. Cal. July 11, 2013) (civil minutes and order granting in part and denying in part defendant's motion for judgment on the pleadings) [hereinafter Minute Order] (dismissing an individual plaintiff's data breach negligence and contract claims against an online video game provider).

111. Minute Order, *supra* note 110, at 13–14.

112. *See* Fleming James, Jr., *Limitations on Liability for Economic Loss Caused by Negligence: A Pragmatic Appraisal*, 25 VAND. L. REV. 43, 43–45 (1972).

113. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013) (holding that Heartland may owe issuer banks a duty of care and may be liable for their purely economic losses); *see also* Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 194–95 (M.D. Pa. 2005) (holding that the direct relationship between a retailer and a card issuer favors imposition of a duty of care).

114. BancFirst v. Dixie Restaurants, Inc., No. CIV-11-174-L, 2012 WL 12879 at *4 (W.D. Okla. Jan. 4, 2012) (holding that no special relationship existed between the parties from which a duty of care would arise); *see also* Dig. Fed. Credit Union v. Hannaford Bros. Co., No. BCD-CV-10-4, 2012 WL 1521479 at *3 (Me.B.C.D. Mar. 14, 2012) (holding that relevant policy considerations militate against imposing a duty of care on a merchant for the benefit of an issuing bank).

115. Defendant's Memorandum of Law in Support of Motion to Dismiss the

and denied most of the motion, stating that plaintiffs had articulated a plausible claim for negligence.[116]

Because courts seem unwilling to find a duty of care in most cases, negligence looks to be an unpromising route for consumers affected by data breaches. With the common law of torts largely precluded by the difficulty of proving a negligence claim, consumers might instead look towards statutory law for relief.

B. Statutory Rights

In the United States, there is no single federal law governing collection and use of personal data.[117] Instead, a patchwork of often-overlapping and contradictory federal and state laws offer the American consumer only partial protection.[118] As the next subsections will discuss, both federal and state lawmakers have attempted to provide consumer protections on a piecemeal basis to address a number of narrow, specific privacy concerns.

1. Federal Statutory Rights

On the federal level, statutes such as the Health Insurance Portability and Accountability Act (HIPAA),[119] the Fair Credit

---

Consolidated Class Action Complaint at *7, *In re* Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522, 2014 U.S. Dist. Ct. Briefs LEXIS 1246 (D. Minn. Sept. 2, 2014).

116. *In re* Target Corporation Customer Data Security Breach Litigation, 64 F. Supp. 3d 1304, 1314 (D. Minn. 2014). Soon after the court's denial, Target settled with consumer plaintiffs for $10 million, and several months later settled with Visa, Inc., for $67 million, with additional settlement talks under way with MasterCard, Inc. Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach Gets Preliminary Approval*, N.Y. TIMES (Mar. 19, 2015), http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0 [http://perma.cc/WEB5-ELC3]; Robin Sidel, *Target to Settle Claims Over Data Breach*, WALL STREET J. (Aug. 18, 2015), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013 [http://perma.cc/976E-SLW2]. Several banks received class certification for their claims in September 2015, making further settlements likely. Joseph Ax, *U.S. Judge Certifies Class Action Over Target Corp Data Breach*, REUTERS (Sept. 15, 2015), http://www.reuters.com/article/2015/09/15/us-target-lawsuit-databreach-idUSKCN0RF2GG20150915 [http://perma.cc/Y8AM-SM9Y].

117. IEUAN JOLLY, PRACTICAL LAW MULTI-JURISDICTIONAL GUIDE 2014/15, DATA PROTECTION IN UNITED STATES: OVERVIEW § 1 (2014).

118. *Id.*

119. 42 U.S.C. §§ 1320d-1 to -9 (2012). HIPAA regulates the use and storage of

Reporting Act,[120] the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act),[121] and the Electronic Communications Privacy Act[122] all give consumers various rights in areas such as health care, consumer credit, and electronic communications. However, none of these acts give consumers explicit statutory rights in regard to data breaches.[123]

There have been recent attempts to address the existing statutory gaps using federal legislation. For example, bills introduced during the 113th Congress included the Personal Data Protection and Breach Accountability Act of 2014,[124] which would have imposed personal data privacy and security requirements on interstate businesses and created both public and private rights of action for violations.[125] Also, the Data Security and Breach Notification Act of 2014 would have directed the Federal Trade Commission (FTC) to promulgate data privacy regulations and establish procedures in the event of a data breach.[126] With few co-sponsors or much attention, in

---

confidential medical information and applies broadly to health care providers and other entities that come in contact with such information. *Id.*

120. 15 U.S.C. §§ 1681–1681x (2012). The Fair Credit Reporting Act applies to consumer reporting entities such as credit bureaus and credit card issuers. *Id.*

121. *Id.* §§ 7702–7704 (2012). The CAN-SPAM Act regulates the collection and use of email addresses and telephone numbers. *Id.*

122. 18 U.S.C. §§ 2510–2522 (2012). The Electronic Communications Privacy Act regulates the interception of electronic communications for targeted advertising. *Id.*

123. One federal statute that does give explicit rights for computer-related crimes is the Computer Fraud and Abuse Act (CFAA). 18 U.S.C. § 1030 (2012). The CFAA allows both criminal penalties and a private civil right of action for unauthorized access to the computer systems of financial institutions, US government computers, or computers used in interstate commerce. *Id.* However, the CFAA largely envisions a direct relationship between a hacker and a breached entity, rather than the collateral relationship of a consumer and a breached entity, and is used increasingly in employer/employee contexts. *Id.*, *see also* Holly R. Rogers and Katharine V. Hartman, *The Computer Fraud and Abuse Act: A Weapon Against Employees Who Steal Trade Secrets*, BLOOMBERGBNA (June 21, 2011), http://www.bna.com/computer-fraud-abuse-act/ [http://perma.cc/LR3V-JWV7]. For consumers affected by a data breach, the CFAA offers little practical redress. *Id.*

124. Meena Harris, *Comparison of Five Data-Breach Bills Currently Pending in the Senate*, INSIDEPRIVACY (Feb. 25, 2014), http://www.insideprivacy.com/united-states/congress/comparison-of-five-data-breach-bills-currently-pending-in-the-senate/ [http://perma.cc/59N4-SDX2].

125. S. 1995, 113th Cong. (2014), https://www.congress.gov/bill/113th-congress/senate-bill/1995/text [https://perma.cc/WSA9-4ZKS].

126. S. 1976, 113th Cong. (2014), https://www.congress.gov/bill/113th-congress/senate-bill/1976 [https://perma.cc/QAB6-TS5L].

part due to strong pushback from industry groups on data regulation in general,[127] both bills face an uncertain future in the new 114th Congress.[128] Furthermore, because the legislation lacks clearly articulated standards for which entities should be subject to liability for data breaches, any consumer seeking redress would still face significant challenges in bringing a claim.[129] The Executive Branch has also attempted to introduce reforms. In 2012, the White House proposed a Consumer Privacy Bill of Rights covering a wide range of privacy-related issues,[130] but the proposal was largely ignored by Congress.[131]

2. State Statutory Rights

While overarching federal regulation is lacking, many state-level laws regulate the collection and use of personal data with potentially far-reaching national effects.[132] Forty-six states, as well as the District of Columbia, Puerto Rico, and the US Virgin Islands, have laws requiring breached entities to

---

127. Kate Tummarello, *'Big Data' Lobbyist: Congress Doesn't Want Online Privacy Law*, THE HILL (Aug. 19, 2014), http://thehill.com/policy/technology/215457-big-data-lobbyist-congress-doesnt-want-online-privacy-law [http://perma.cc/5HJP-SRXR]. Most opposition is aimed at avoiding regulations that would interfere with the vast amounts of marketing data currently collected and used by retailers and others, with lobbyists "[p]ushing back on calls for a sweeping consumer privacy law in a 'big data' era where companies can collect, analyze, and share large amounts of information about consumers." *See id.*

128. Senate Bills 1976 and 1995 had only three co-sponsors each. Both bills were introduced by Democratic sponsors while their party held a majority in the chamber and have not been reintroduced in the 114th Congress.

129. *See* Harris, *supra* note 124.

130. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (2012).

131. Tom Hamburger, *Consumer Privacy Rights Need Urgent Protection in Washington, Activists Say*, WASH. POST (Feb. 24, 2014), http://www.washingtonpost.com/politics/consumer-privacy-rights-need-urgent-protection-in-washington-activists-say/2014/02/24/1764ba22-9cb7-11e3-975d-107dfef7b668_story.html [http://perma.cc/PWM4-HZ7U].

132. *Id.* For example, the California Online Privacy Protection Act was amended in 2013 to require commercial websites and online services, wherever located, to disclose how they respond to "do-not-track" requests and whether third parties collect personally identifiable information from consumers. *California Amends Online Privacy Policy Law to Require Tracking Disclosures*, PRIVACY & INFO. SEC. L. BLOG, HUNTON & WILLIAMS (Sept. 30, 2013), https://www.huntonprivacyblog.com/2013/09/30/california-amends-online-privacy-policy-law-to-require-tracking-disclosures/ [https://perma.cc/R8SM-KP76].

notify affected consumers in the case of a security breach involving personal information.[133] At least thirty-two states and Puerto Rico have passed laws requiring entities holding personal information to destroy, dispose of, or otherwise make it unreadable or undecipherable after a stated period or event.[134]

Most states have not enhanced their data breach notification statutes with private civil rights of action that consumers could use to recover damages for notification failures.[135] Only eleven states currently provide an explicit private right of action to file suit against companies that violate notification provisions.[136] However, no states have created a private right of action for data breaches in general.[137] Because of its near universality, the lack of private rights of action could be considered a statutory choice by state lawmakers across the country.

3. Private Rights of Action

A private right of action allows injured parties to sue on their own behalf for damages caused by another's violation of federal or state statutes,[138] rather than rely on public enforcement by authorities who may be unable—or unwilling—

133. Reid J. Schar & Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, 12 PRIVACY & SECURITY L. REP. (BNA) 1381, 12 PVLR 1381 (BL) (Aug. 12, 2013). *See, e.g.*, CAL. CIV. CODE §§ 1798.80, 1798.82, 1798.84 (West 2012); COLO. REV. STAT. § 6-1-716 (2014); DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2015); MASS. GEN. LAWS ch. 93H-1, §§ 1–6 (2014); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2013); TEX. BUS. & COM. CODE ANN. § 521 (West 2015).

134. *Data Disposal Laws*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx [http://perma.cc/52AV-7ZDD]. *See, e.g.*, CAL. CIV. CODE § 1798.81 (West 2012) (requiring that reasonable disposal steps be taken when customer records are no longer retained by a company doing business in California).

135. *E.g.*, COLO. REV. STAT. § 6-1-716 (2014). The Colorado Consumer Protection Act gives the state Attorney General the right to bring an action to address violations, but does not provide a private right of action. *Id.*

136. Schar & Gibbons, *supra* note 133. The states are: Alaska, California, Louisiana, Maryland, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Virginia, and Washington. *Id.*

137. *See id.*

138. *See* Donna L. Goldstein, *Implied Private Rights of Action Under Federal Statutes: Congressional Intent, Judicial Deference, or Mutual Abdication?*, 50 FORDHAM L. REV. 611, 614 (1982).

to bring cases for the benefit of a single individual.[139] Available under a variety of federal and state statutes, either expressly in law or impliedly via judicial construction, the private right of action has developed perhaps most strongly in the federal securities law context, allowing financially injured investors to sue for violations of federal securities laws.[140] Private rights of action can act as a secondary judicial enforcement mechanism for federal regulatory efforts,[141] and in a data breach context could act as a crucial tool for ameliorating the problems that consumers and businesses alike face when bringing tort claims.[142]

Private rights of action are not without controversy, however, with some observers claiming that they could "become a one-sided litigation machine" or "lead to a new litigation industry."[143] While these concerns are not without merit, they

---

139. *See* William E. Kovacic, Gen. Counsel, Fed. Trade Comm'n, Private Participation in the Enforcement of Public Competition Laws, Speech at British Institution of International & Comparative Law's Third Annual Conference on International and Comparative Competition Law: The Transatlantic Antitrust Dialogue (May 15, 2003), https://www.ftc.gov/public-statements/2003/05/private-participation-enforcement-public-competition-laws [https://perma.cc/6WM7-7VB2] ("Private rights of action diminish, if not eliminate, the gate-keeping authority of public prosecutors and reduce their ability to control the development of policy by their selection of cases. Specifically, independent private rights to prosecute deny prosecutors the capacity to modulate the law's application by deciding to prosecute some violations more aggressively and prosecute other offenses less vigorously.").

140. Most notably, private actions are routinely brought under Section 10 of the Securities Exchange Act of 1934, codified at 15 U.S.C. § 78j (2012), and Rule 10b-5, promulgated thereunder. Rule 10b-5 states, in part, that "it shall be unlawful for any person, directly or indirectly, . . . (a) to employ any device, scheme, or artifice to defraud, (b) to make any untrue statement of a material fact or to omit to state a material fact . . . , or (c) to engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security." 17 C.F.R. § 240.10b-5 (2015). Investors can use Rule 10b-5 (and its judicially implied private right of action) to seek redress for financial damages and losses caused by, among other violations, insider trading, false or misleading public statements by corporate officers, and deceptive investment prospectuses. For the elements of a private 10b-5 claim, *see* Thomas M. Madden, *Significance and the Materiality Tautology*, 10 J. BUS. & TECH. L. 217, 218–19 (2015).

141. *See* Kovacic, *supra* note 139 ("[P]rivate rights of action magnify the role of the courts in implementing the law. In a world of multiple potential prosecutors, public and private, the courts become the chief vehicle for defining the law's content. The rulings of adjudicatory tribunals . . . assume greater importance in shaping competition policy.").

142. *See* discussion *supra* Section II.A.

143. Letter from Am. Express Co. et al. to the Chairman and Ranking Member of U.S. Senate Comm. on the Judiciary, (May 25, 2011), http://www.protect

tend to minimize the role of the judiciary in limiting private rights of action. The Supreme Court, for example, established clear guidelines for finding implied private rights of action some forty years ago.[144] Indeed, the Court's recent decisions narrowing long-standing implied private rights of action for securities violations[145] only reinforce the judiciary's skepticism of implied private rights of action. As for express private rights of action, careful legislative drafting can address many potential problems, and the judiciary can employ its traditional tools of statutory construction to resolve any unforeseen issues that arise. Until a private right of action exists for data breaches, injured consumers must turn to other sources for a remedy.

C. Regulatory Law: Section 5 and the FTC

Faced with a lack of statutory solutions at the national level, the Federal Trade Commission (FTC) has started to fill in the gaps between industry-specific privacy laws, such as HIPAA and the Fair Credit Reporting Act,[146] by using the authority granted to it under Section 5 of the Federal Trade

innovation.com/pdf/opposition/16-may_25_2011_net_coalition.pdf [http://perma.cc/6QVF-TX59]. The signatories, including American Express, Discover, Visa, Yahoo!, eBay, and Google, opposed a proposed private right of action that would have allowed copyright or trademark owners to bring suit against an Internet domain name associated with infringing activity. *See also PCI Expresses Opposition to Overhaul of CT Unfair Insurance Practices Act*, PROP. CASUALTY INSURERS ASS'N OF AM. (Feb. 5, 2009), https://www.pciaa.net/pciwebsite/Cms/Content/ViewPrint?sitePageId=8964 [https://perma.cc/HAE8-PBF5] (opposing a proposed private right of action for violation of Connecticut state insurance law); Eric Dowdy, *Assisted Living Legislation on Governor Brown's Desk*, LEADINGAGE CALIFORNIA (Sept. 10, 2014), http://engageheadlines.com/assisted-living-legislation-on-governor-browns-desk/ [http://perma.cc/NHK4-6MLD] (crediting industry opposition for the removal of a private right of action from a California assisted living reform bill).

144. Cort v. Ash, 422 U.S. 66, 78 (1975).

145. *See* Santa Fe Indus., Inc. v. Green, 430 U.S. 462 (1977) (holding that Rule 10b-5 is not applicable to breach of corporate fiduciary duty involving neither manipulation nor deception); Piper v. Chris-Craft Indus., Inc., 430 U.S. 1 (1977) (holding that §10(b) is not applicable to misrepresentation by competing tender offeror); Ernst & Ernst v. Hochfelder, 425 U.S. 185 (1976) (holding that §10(b) and Rule 10b-5 are not applicable to negligent misstatements or omissions); Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723 (1975) (holding that §10(b) and Rule 10b-5 are not applicable to plaintiffs who are neither purchasers nor sellers of securities).

146. *See supra* Section II.B.1.

Commission Act (FTC Act).[147] Section 5 gives the FTC broad authority to prohibit "unfair or deceptive acts or practices in or affecting commerce."[148] The FTC has been increasingly aggressive in privacy and data security contexts, investigating a wide variety of "unfair" and "deceptive" practices.[149] Since 2011 the FTC has brought dozens of enforcement actions against companies accused of violating consumer privacy or mishandling consumer data; most companies have settled rather than risk litigating FTC charges.[150] FTC enforcement actions under Section 5 of the FTC Act fall under two main prongs: deceptiveness and unfairness. This Comment will discuss both of the prongs, as well as criticisms of the FTC's Section 5 enforcement efforts, in the following subsections.

1. The Deceptiveness Prong of Section 5

The FTC maintains that a data breach involving a company's failure to adhere to its own stated data security policies is deceptive within the meaning of Section 5 because it wrongly leads consumers to believe that their data is being handled securely.[151] By encouraging companies to implement proper privacy and data security policies at every stage of development, the FTC seeks to ensure that consumers can rely on privacy policies when deciding to give private information to a company and when developing privacy expectations for the relationship.[152]

Deceptiveness actions usually accompany other FTC charges. The FTC often brings enforcement actions under

147. Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, A.B.A., http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html [http://perma.cc/4CPV-CJGU].

148. Federal Trade Commission Act § 5(a), 15 U.S.C. § 45(a)(1) (2012).

149. Woods, *supra* note 147.

150. Wendy Davis, *Appeals Court Agrees to Hear Wyndham's Challenge to FTC*, ONLINE MEDIA DAILY (July 30, 2014), http://www.mediapost.com/publications/article/231080/appeals-court-agrees-to-hear-wyndhams-challenge-t.html [http://perma.cc/C9LZ-CSKH]. For example, in 2014 the FTC settled data security cases against Snapchat, Fandango, and Credit Karma, among others. FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [https://perma.cc/K7HP-3MJ7].

151. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012).

152. *Id.*

violations of stand-alone statutory privacy laws that then result in deceptive acts under Section 5.[153] In 2012, the FTC settled a civil complaint against an Illinois payday loan provider who tossed sensitive customer information into the trash, thus violating, among other statutes, the Disposal Rule of the Fair Credit Reporting Act (FCRA).[154] The FTC alleged that the payday lender's FCRA violations constituted deceptive acts in violation of Section 5.[155] Rather than contest the charges, the payday lender settled and agreed to $101,500 in fines, twenty years of third-party privacy auditing, and twenty years of FTC monitoring.[156] While the FTC's deceptiveness actions serve an important role in regulating companies dealing with sensitive consumer information, this regulation only indirectly benefits consumers themselves.

2. The Unfairness Prong of Section 5

The FTC is also working to develop a line of authority under the unfairness prong of Section 5. In the active test case of *FTC v. Wyndham Worldwide Corp.*, litigation arose in connection with three separate breaches of Wyndham hotel and resort networks, allegedly due to poor security practices.[157] The breaches compromised more than 619,000 guest card numbers and resulted in more than $10.6 million in fraudulent losses.[158] The FTC alleged that Wyndham's "actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition and, . . . therefore, [Wyndham]'s acts and practices . . . constitute unfair acts or practices" under Section 5.[159] Wyndham moved to dismiss the unfairness claim, contending that the FTC was not "authorize[d] . . . to generally establish data-security standards

153. Woods, *supra* note 147.

154. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief ¶ 20, United States v. PLS Fin. Servs., No. 1:12-cv-8334 (N.D. Ill. Oct. 17, 2012).

155. *Id.* ¶ 31.

156. Stipulated Final Judgment and Order for Payment of Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5, 9, 12, United States v. PLS Fin. Servs., No. 1:12-cv-8334 (N.D. Ill. Oct. 26, 2012).

157. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 608–09 (D.N.J. 2014).

158. *Id.* at 609.

159. *Id.* at 610.

for the private sector under Section 5."[160] The district court found the argument unpersuasive, rejecting Wyndham's "request to carve out a data-security exception to the FTC's authority" and denying the motion to dismiss.[161] However, due to the novelty of the FTC's unfairness theory in a data breach context, the district court gave Wyndham leave to request an interlocutory appeal on the issue.[162] The Third Circuit Court of Appeals heard oral arguments in the case in March 2015,[163] and many observers thought the court was unimpressed by the FTC's data breach unfairness theory.[164] In a somewhat surprising result, the panel unanimously upheld the FTC's authority to bring unfairness actions for data breaches, handing the FTC a resounding victory for its theory and

---

160. *Id.* at 611.

161. *Id.* at 615.

162. *Id.* at 636. The district court certified the following questions to the Third Circuit Court of Appeals:

> (1) Whether the Federal Trade Commission can bring an unfairness claim involving data security under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a); and, (2) Whether the Federal Trade Commission must formally promulgate regulations before bringing its unfairness claim under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Id.

163. Katherine Gasztonyi, *Wyndham Oral Argument: Third Circuit Expresses Doubt About FTC's Data Security Authority*, INSIDE PRIVACY (Mar. 3, 2015), http://www.insideprivacy.com/united-states/federal-trade-commission/recap-of-oral-argument-in-ftc-v-wyndham/ [http://perma.cc/6PEA-N775].

164. *See id.* ("The court also spent considerable time on the subject of whether the FTC placed companies on notice on what it believed would constitute reasonable or unreasonable cybersecurity standards. The FTC said that the complaints and consent decrees published on the FTC's website put companies on notice as to what constituted unreasonable security standards. . . . The court appeared to be unconvinced by this argument, despite FTC's statement that any careful general counsel should be looking at what the FTC is doing."); Archis A. Parasharami, *Third Circuit Hears Oral Argument Over Whether FTC Has Authority to Regulate Data Security*, CLASS DEFENSE BLOG (Mar. 6, 2015), http://www.classdefenseblog.com/2015/03/third-circuit-hears-oral-argument-over-whether-ftc-has-authority-to-regulate-data-security/ [http://perma.cc/3H5A-EF6M] ("It is always perilous to read the tea leaves after an oral argument. But it is an understatement to say that the Third Circuit's panel was dropping some hints, especially by requesting further briefing on whether the FTC action [even] belongs in federal court."); Stacey Brandenburg, *Third Circuit Examines FTC's Role in Data Security Space*, ZWILLGEN BLOG (Mar. 6, 2015), http://blog.zwillgen.com/2015/03/06/third-circuit-examines-ftcs-role-data-security-space/ [http://perma.cc/D9T8-G2F9] ("The court's questioning took a skeptical tone in probing, as a threshold matter, whether Congress imbued the FTC (which has authority to investigate and pursue claims of unfairness under Section 5(a)) with the authority to define or declare specific practices as 'unfair.'").

remanding the case for further proceedings.[165] While any new actions brought under *Wyndham*'s unfairness theory may help regulate future data privacy, they will still benefit consumers only indirectly.

3. Criticisms of FTC Enforcement Under Section 5

Although the FTC's aggressive enforcement actions do seem to be a possible answer to the current lack of statutory data privacy rights, the efficacy of the agency's efforts is uncertain and its use of Section 5 authority in a data breach context is controversial.[166] Most criticisms of FTC action focus on the agency's regulatory authority (or lack thereof) to oversee data security.[167] Others claim that the "FTC's regulation of business systems by decree threatens to stifle innovation by companies related to data security and to impose costs that will be passed on in part to consumers" and that "[m]issing from the . . . decree calculus is the question of whether the benefits in diminished data security breaches justify [the] costs."[168] Even the House Committee on Oversight and Government Reform has expressed concern about the FTC's data breach enforcement methods, questioning whether a particular FTC action "aided a company whose business practices allegedly involve disseminating false data about the nature of data security breaches."[169]

---

165. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 244–47, 249, 255–59 (3d Cir. 2015).

166. *See, e.g.*, Kashmir Hill, *The FTC's Controversial Battle to Force Companies to Protect Your Data*, FORBES (Aug. 21, 2014), http://www.forbes.com/sites/kashmirhill/2014/08/21/the-ftcs-controversial-battle-to-force-companies-to-protect-your-data/ [http://perma.cc/36EV-C75B].

167. *Id.*

168. Alden F. Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, HERITAGE FOUND. (Sept. 10, 2014), http://www.heritage.org/research/reports/2014/09/the-federal-trade-commissions-role-in-online-security-data-protector-or-dictator [http://perma.cc/XWQ6-STWY].

169. Letter from Chairman Darrell Issa to the FTC Acting Inspector General, House Comm. on Oversight & Gov't Reform 3 (Jun. 17, 2014), http://oversight.house.gov/wp-content/uploads/2014/06/2014-06-17-DEI-to-Tshibaka-FTC-IG-Lab MD-Tiversa.pdf [http://perma.cc/H467-FFAD]. The Chairman was concerned with the FTC's relationship to the source of information about the data breach involved in the *LabMD* data breach litigation. *See In re* LabMD, Inc., No. 9357 (Fed. Trade Comm'n, Aug. 29, 2013), http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf [http://perma.cc/9LRW-5WNE]. According to reports, it appears that the FTC's LabMD enforcement action relied almost entirely upon records and other evidence of poor data security practices at LabMD

Perhaps more salient are critiques that FTC actions give businesses little or no guidance about what exactly constitutes a reasonable level of privacy and data security.[170] The FTC has been "particularly tight-lipped about what data security standards it expects" companies to employ, and a "chorus of lawyers and scholars have complained that enforcement is misguided absent clearer . . . standards."[171] Because the FTC relies on the statutory language of Section 5 instead of promulgating clear standards via notice-and-comment rulemaking, "anyone seeking to design a program that complies with FTC expectations would have to . . . parse out what the FTC views as '*un*reasonable'—and, by negation, reasonable—privacy and data security procedures" from FTC complaints.[172]

While reverse-engineering the FTC's definition of reasonable privacy and data security offers "neither a safe harbor from enforcement nor immunity from a . . . data security breach," it does offer a starting point to clear up the uncertainty surrounding Section 5 compliance.[173] Without Congressional action, however, the business community and the FTC itself will ultimately have to rely on judicial interpretation of Section 5. Such interpretation may provide more concrete guidance than the FTC currently offers, but will still leave consumers largely unprotected. No matter how clear or certain, FTC regulations under either the deceptiveness or

---

that were, in fact, fabricated by Tiversa, an Internet security firm, after LabMD spurned its service offering. Marianne Kolbasuk McGee, *Bombshell Testimony in FTC's LabMD Case*, DATA BREACH TODAY (May 8, 2015), http://www.databreachtoday.com/bombshell-testimony-in-ftcs-labmd-case-a-8212 [http://perma.cc/H94H-UF58]. It was apparently Tiversa's business practice to make it appear that prospective clients' files were spread among websites of known identity thieves. *Id.* The websites, however, were actually for computers that were already shut down by law enforcement. *Id.* In essence, Tiversa "made up the story it gave to the FTC out of whole cloth." *Id.*

170. Patricia Bailin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, INT'L ASS'N OF PRIVACY PROFS. WESTIN RES. CTR. (Sept. 19, 2014), https://privacyassociation.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices/ [https://perma.cc/3WJX-DBVF].

171. *Id.*

172. *Id.* The IAPP Westin Research Center study analyzed forty-seven FTC privacy and data security cases since 2002 and extrapolated seven categories that appear to concern the FTC most: Privacy, Security, Software/Product Review, Service Providers, Risk Assessment, Unauthorized Access/Disclosure, and Employee Training. *Id.* The study then deduced concrete steps that companies might take to avoid Section 5 liability. *Id.*

173. *Id.*

the unfairness prong of Section 5 will never directly benefit consumers affected by data breaches. As Part III discusses, consumers necessarily need alternatives to the FTC's statutory enforcement efforts.

III. ENHANCING CONSUMER RIGHTS AND REMEDIES

Consumers victimized by a data breach are at a severe disadvantage under current law. With courts unwilling to recognize the duty of care required by tort law, Congress unlikely to strengthen the patchwork of statutory law, and the FTC's murky authority in regulatory law, the average consumer is essentially at the mercy of a breached entity's largesse to gain any recompense for stolen data. Unfortunately, that recompense is usually limited to well-publicized offers of free credit monitoring, a service so poorly tailored to addressing consumer data breaches that one expert characterized it as "retailer[s] telling their customers to bug off."[174] As another expert pointed out, "[c]redit monitoring does nothing to identify or alert you when someone has compromised your existing payment information . . . that type of fraudulent activity does not show up on a credit report, so credit monitoring is woefully inadequate."[175]

While credit monitoring will alert consumers to new accounts opened in their name, and may therefore be somewhat useful for some data breaches, fraudulent credit card use will not show up on a credit report because only account-level information is shown, not individual charges.[176] Furthermore, credit reports are concerned with a consumer's past credit delinquencies and payment history, not what kind of purchases are currently being made.[177] Perhaps most critically, debit card information is not shown on a credit report at all.[178] It is quite clear, then, that American consumers need more than essentially pointless monitoring services to make good the damages of data breaches.

---

174. Gregory Karp, *Why Credit Monitoring Will Not Help You After a Data Breach*, CHI. TRIB. (Aug. 15, 2014), http://www.chicagotribune.com/business/breaking/chi-why-credit-monitoring-will-not-help-you-after-a-data-breach-20140815-story.html [http://perma.cc/B5Y9-2LPA].

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.*

One path towards improving consumer remedies for data breaches, and away from the useless public relations measures that are credit monitoring services, may be found in the data protection principles used for decades across the Atlantic. The European Union (EU) has identified seemingly workable strategies to address consumer data breaches. These strategies could be imported relatively easily into the United States and adapted to the distinct requirements of American law. The following sections discuss the principles of EU data privacy law, propose a framework for adapting them to US law, and address possible challenges to enhancing consumer rights and remedies in this manner.

A. London Calling

In contrast to the laissez-faire approach to privacy and data security embraced by American law, the EU has been far more focused on providing its citizens with fundamental privacy protections. Adopted in 1995, the EU Data Protection Directive (Directive)[179] harmonized data protection laws already existing in several EU member states and was intended to strictly protect individuals "with regard to the processing of personal data and . . . the free movement of such data."[180] Ratified in 2009, the Charter of Fundamental Rights of the EU explicitly states that "[e]veryone has the right to the protection of personal data concerning him or her,"[181] thus obligating member states and institutions to observe and guarantee this right when implementing EU law.[182] The Directive addresses data protection by defining personal data, dividing the parties responsible for data protection into two categories, and imposing notification requirements for uses of personal data.

EU law defines personal data very broadly as "any

179. Council Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) [hereinafter Directive].

180. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 17 (2014), http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf [http://perma.cc/J6PY-WNEB] [hereinafter HANDBOOK].

181. Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326).

182. HANDBOOK, *supra* note 180, at 18.

information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his . . . identity."[183] This means that information often thought to be innocuous by Americans, such as names and phone numbers, is regarded as protected personal data in Europe.

The Directive divides parties responsible for data protection into two categories: data controllers and data processors.[184] A controller is defined as "the natural or legal person . . . which . . . determines the purposes and means of the processing of personal data."[185] A processor is defined as "a natural or legal person . . . which processes personal data on behalf of the controller."[186] The Directive contemplates a fairly straightforward relationship between the controller and the processor.[187] For example, in this regime a company such as Target that collects credit card information in order to accept customer payments would be considered a data controller, while a payment processor who authenticates the payments at Target's request would be a data processor. In practice, the relationship is far more complicated, especially when considering the complex joint processing activities that exist amongst large multinational corporations, and the Directive's inflexibility does not easily cope with the networked nature of modern business transactions.[188]

The Directive provides robust notification provisions for data processing, requiring controllers to notify a local supervisory authority, usually a privacy ministry or similar office created by each EU member country, before executing

183. Directive, *supra* note 179, at Art. 2(a).

184. Lokke Moerel, *Back to Basics: When Does EU Data Protection Law Apply?*, 1 INTL. DATA PRIVACY LAW 92, 98–99 (2011), http://idpl.oxfordjournals.org/content/1/2/92.full.pdf+html [http://perma.cc/378M-8EZC].

185. Directive, *supra* note 179, at Art. 2(d).

186. *Id.* at Art. 2(e).

187. Moerel, *supra* note 184.

188. NEIL ROBINSON, ET AL., RAND EUROPE, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 36 (2009) ("The relationship between processor and data controller envisaged in the Directive does not adequately cover all the entities involved in the processing of personal data in a modern networked economy. There is uncertainty about when a processor becomes a controller or vice versa, particularly in an online environment where the act of visiting a website might result in cookies being sent from a number of sources scattered around the globe.").

many processing operations.[189] It also provides strong remedies for persons affected by a breach of data protection rights, including judicial remedies, controller liability, and sanctions for infringement of data protection provisions, although the Directive offers no specific guidance on the actual penalties.[190]

The EU data protection regime is not without controversy, especially for US technology companies. Most prominently, Google has run afoul of EU regulators over operations such as the Street View mapping service.[191] In addition, the recent European Court of Justice (ECJ) ruling regarding Google searches and the "right to be forgotten" online has the potential to fundamentally harm how the Internet works worldwide.[192]

---

189. Directive, *supra* note 179, Art. 8.

190. *Id.* at Arts. 22–24; *see also* Archana Venkatraman, *Only One in 100 Cloud Providers Meet Latest EU Data Protection Requirements*, COMPUTER WEEKLY (Aug. 12, 2014), http://www.computerweekly.com/news/2240226620/Only-one-in-100-cloud-providers-meet-new-EU-data-protection-requirements [http://perma.cc/GY2F-Z4M6]. The Draft European Union General Data Protection Regulation expected to come into effect in 2015 requires data controllers and data processors to share liability for breaches and violations of the law, and imposes penalties of up to five percent of a company's annual revenue, up to €100 million. *Id.*

191. Frances Robinson, *U.S. Surveillance Programs Spur EU Efforts to Tighten Data Protection Rules*, WALL STREET J. (Aug. 8, 2013), http://online.wsj.com/articles/SB10001424127887324522504579000702411343532 [http://perma.cc/R2UZ-8WCQ].

192. Jeffery Toobin, *The Solace of Oblivion*, NEW YORKER (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion [http://perma.cc/98PF-LMBA]. In 2014, the ECJ ruled against Google in a case related to a Spanish businessman's request to remove a link to a newspaper announcement of his past foreclosure proceeding. *See* Case C-131/12, Google Spain SL, Google Inc., v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Celex No. 612CJ0131 (May 13, 2014). The proceeding had concluded in 1998, but the businessman found links to the announcement while googling his name in 2009. *Id.* He argued that the information was no longer relevant and should be deleted, while Google argued that he did not have the right to erase lawfully published material. *Id.* In agreeing with the businessman the ECJ held that a search engine must remove links to third party information that an individual believes to be "inadequate, irrelevant or no longer relevant, or excessive" in relation to the purposes for which it was originally posted. *Id.* The ECJ decision provoked withering criticism in the US and UK, with the House of Lords calling the decision "misguided in principle and unworkable in practice." Toobin, *supra.* Although Google has complied with the ruling in relation to regional European search domains, such as www.google.es (Spain), www.google.fr (France), or www.google.de (Germany), the company has not extended it to the main Google search domain, leading to conflicts with European regulators that interpret the ECJ ruling as applying worldwide. *Id.*; Mark Scott, *France Wants Google to Apply 'Right to Be Forgotten' Ruling Worldwide or Face Penalties*, N.Y. TIMES: BITS (June 12, 2015), http://bits.blogs.nytimes.com/ 2015/06/12/french-regulator-wants-google-to-apply-right-to-be-forgotten-ruling-worldwide/ [http://perma.cc/AJ84-XU9Z]. Further discussion of the issue is beyond the scope of this Comment, but

The root of the ECJ's decision and the subsequent controversy over the decision in the US can be traced to very different ideas about privacy in America and Europe.[193] Recent historical experience with political systems including fascism and communism, both of which used pervasive surveillance states to strengthen the control of totalitarian governments, causes Europeans to be wary of *any* collection of personal data for *any* use.[194] "In Europe, the right to privacy trumps freedom of speech; the reverse is true in the United States."[195] Americans regard free speech as overriding privacy concerns for all but a few categories of information because, in the United States, the value of free expression is considered more important than individual privacy.[196]

B. Importing EU Data Protection Principles into American Law

Despite the very different concepts of privacy that exist in Europe and the United States, the principles of data protection embodied in the Directive can be instructive in providing American consumers with greater protection from data breaches. Analysis of the Directive's principles can distill them into three salient concepts that can be adopted via legislation: (1) elements of personally identifiable data; (2) entities controlling or processing that data; and (3) liability for misuse of data.

1. Elements of Personally Identifiable Data

Elements of personally identifiable data (PID) are already found in existing American privacy laws such as HIPAA[197] and the FCRA.[198] Pending legislation also includes extensive definitions of "sensitive personal information" or "personal

---

the "right to be forgotten" raises fascinating and troubling questions regarding personal privacy, freedom of speech, the application of national law to international entities, and who actually gets to regulate the Internet.

193. Toobin, *supra* note 192.

194. *Id.*; *see generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

195. Toobin, *supra* note 192.

196. *Id.*

197. 45 C.F.R. § 106.103 (2014) (defining individually identifiable health information).

198. 15 U.S.C. § 1681a(d)(1) (2012).

information."[199] From a consumer point of view, a useful definition of PID would incorporate the general contours of EU law while narrowing them to exclude information that Americans do not find overly private. For example, PID might be defined as follows: *'personally identifiable data' means any personal, medical, financial, consumer, or other data that can: (1) identify an individual, or (2) be used in connection with any other data to identify an individual; and that (3) would be considered sensitive personal information by a reasonable individual.*

This would both incorporate and consolidate the concepts of PID found in current federal definitions.[200] It narrows the seemingly limitless definition of PID found in European law[201] by adding a restriction based on the well-known "reasonable person" standard from tort law,[202] while still incorporating a more European concept of privacy than currently exists in American law. This would give consumers and courts more flexibility to deal with the injuries associated with data breaches, while still allowing businesses to collect and use data considered innocuous by most American consumers, such as email addresses, phone numbers, and even the consumer purchasing data obtained from supermarket discount cards.

2. Entities Controlling or Processing Data

Missing from current American law is the European concept of data controllers and data processors. Creating clear standards for what kind of entity is subject to data privacy liability is essential for any reform, but currently proposed

199. *See* Harris, *supra* note 124.

200. *See, e.g.*, 45 C.F.R. § 106.103; 15 U.S.C. § 1681a(d)(1).

201. *Cf.* Directive, *supra* note 179, at Art. 2(a) (defining PID as "any information relating to an identified or identifiable natural person.").

202. Alan D. Miller & Ronen Perry, *The Reasonable Person*, 87 N.Y.U. L. REV. 323, 325–26 (2012) ("The reasonable person test is the traditional test for compliance with the duty of care in torts. Negligence arises from doing an act that a reasonable person would not do under the circumstances, or from failing to do an act that a reasonable person would do. . . . The standard, therefore, is the level of care that would be exercised under the same or similar circumstances by 'the great mass of mankind'—that is, the 'generally accepted standard.' This is a positive definition of reasonableness, in the sense that it derives from reality rather than from morality. According to this test, a person's conduct is deemed unreasonable if people actually consider it so, . . . [a]nd it is deemed reasonable if people (or a certain portion of them) believe the conduct to be so.").

legislation falls short on that front.[203] Controllers might be defined as *the person or legal entity who collects, stores, and processes personally identifiable data.*[204] A processor might be defined as *the person or legal entity who receives personally identifiable data from a controller for collection, storage, or processing.*[205] These definitions focus on the relationship between the consumer and the entity acquiring data, or on the relationship between the acquirer and the entity receiving acquired data, rather than on the relationship between the entity and the data. Focusing on the relationship between the consumer and the controller, or between the controller and the processor, makes these definitions expansive enough to cover almost any possible type of transactional relationship involving PID. Essentially, the identity of the entity does not matter: all that matters is their relationship to the source of the data. Due to the distributed nature of data storage and processing by modern corporations, a single entity may necessarily fall under both definitions, but this overlap would simply serve to confirm an entity's potential liability.

While it may seem somewhat duplicative to have separate definitions for entities that may perform essentially the same operations, both definitions are necessary to capture a range of potential uses of PID, including some that have likely not even been invented yet. The existence of dual definitions will also reduce the chance that a data controller might attempt to avoid liability by passing collected data to a third party, and also ensure that a data controller is not unjustly held liable for the bad acts of a data processor. If these standards had applied to Target during the 2013 breach, then consumers would have had little trouble identifying the company as a data controller, thus providing a clearly liable party to provide redress for the consumers' injuries.[206] This would also avoid difficulty with the often complex relationships among corporate parents and subsidiaries by making it clear that the key characteristics are who holds the data and who receives it from the holder.

---

203. *See* Harris, *supra* note 124.

204. *Cf.* Directive, *supra* note 179, at Art. 2(d) (defining controller as "the natural or legal person . . . which . . . determines the purposes and means of the processing of personal data.").

205. *Cf.* Directive, *supra* note 179, at Art. 2(e) (defining processor as "a natural or legal person . . . which processes personal data on behalf of the controller.").

206. *See supra* Section I.C.

3. Liability for Misuse of Data

Finally, statutory liability for misuse of data should be part of any reform. First, creating a federal private right of action[207] and a statutory duty of care between consumers, controllers, and processors would eliminate the problems that consumers and businesses alike face when bringing tort claims.[208] Second, statutory reform should explicitly incorporate the principal that a data breach is a cognizable injury in and of itself, even if no immediate monetary damages have occurred, and that no direct relationship is required in a retailer-consumer relationship. However, it must be noted that any statutory reform should not impose strict liability for data breaches on any party. Instead, the standard of care should be one of reasonableness under the totality of the circumstances (i.e., a retailer accepting credit cards should have a higher standard of care than a company collecting only names and email addresses). Cybersecurity is a constantly evolving technology, and endlessly inventive hackers are unlikely to stop finding new ways to attack and breach corporate networks. Holding companies liable for data breaches even when, unlike Target, they did everything reasonably possible to prevent a breach would not encourage responsible data security and could even hamper our current electronic exchange economy. Third, a governing body for data privacy regulation should assist consumers and businesses in setting expectations and guidelines with regard to security. Since the FTC has already shown a willingness to accept the task,[209] it would be logical to expand Section 5 authority to expressly encompass privacy and data security and to direct the FTC to promulgate appropriate regulations. Taken together, these three proposals would significantly enhance consumer rights and remedies for data breaches.

If these proposals had been in place prior to the Target breach, they would have eliminated legal barriers to the individual consumer plaintiff's claims and facilitated the corporate plaintiffs' ability to pursue remedies. First, a federal private right of action would have given consumers a clear cause of action for their Target data breach claims. Second,

207. *See supra* Section II.B.3.
208. *See supra* Section II.A.
209. *See supra* Section II.C.

statutory reforms would have eased (but not eliminated) both the consumer plaintiffs' and the corporate plaintiffs' burdens of proof with regard to injury from the Target breach, as well as defined the retailer-consumer relationship necessary to show an injury. Finally, granting the FTC explicit privacy and data security regulatory authority under Section 5 would have given consumers, other corporations, and Target clear expectations with regard to preventing and responding to data breaches.

C. Challenges to Enhancing Consumer Rights and Remedies

Legal change does not happen in a vacuum, and data security reform is no different. While there is some hope of federal reform legislation emerging from Congress,[210] the reality of our current divided government might scuttle any attempts to improve consumer data security protections. Efforts to address US cybersecurity in the wake of Edward Snowden's revelation of classified intelligence programs[211] have

---

210. *See* Natasha Singer, *Data Protection Laws, an Ocean Apart*, N.Y. TIMES (Feb. 2, 2013), http://www.nytimes.com/2013/02/03/technology/consumer-data-protection-laws-an-ocean-apart.html [http://perma.cc/SPF6-QLXT].

211. *See generally Edward Snowden: Leaks That Exposed US Spy Programme*, BBC (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964 [http://perma.cc/X46J-P64S]; Matt Sledge, *One Year After Edward Snowden's Leaks, Government Claims of Damage Leave Public in Dark*, HUFFINGTON POST (June 5, 2014), http://www.huffingtonpost.com/2014/06/05/edward-snowden-damage_n_5448035.html [http://perma.cc/LZC4-ESJN]. Edward Snowden became disaffected with American intelligence programs after learning the scope and pervasiveness of US Internet and telephone surveillance while working as a systems analyst for the Central Intelligence Agency in the mid-2000s. *Profile: Edward Snowden*, BBC (Dec. 5, 2013), http://www.bbc.com/news/world-us-canada-22837100 [http://perma.cc/C8QT-T32V]. Snowden later took a job as an IT contractor with the National Security Agency (NSA), apparently with the express intention of stealing classified material for later public disclosure. *Id.* Using the high-level administrator access to NSA networks granted by his position, Snowden copied hundreds of thousands of secret documents detailing dozens of classified surveillance programs, including NSA collection of telephone records from tens of millions of Americans, British tapping of transatlantic fiber-optic cables, and US monitoring of communications between European heads of government. *Edward Snowden: Leaks That Exposed US Spy Programme*, *supra*. He then travelled to Hong Kong and, in June 2013, began leaking the documents to reporters from the Guardian and the Washington Post. *Id.* Snowden's revelations sent seismic shockwaves throughout the international intelligence community, frayed US relations with numerous foreign governments, and led to considerable domestic outcry. *Id.* Even US economic interests have been adversely affected, with American technology companies estimating $35 billion in future business lost abroad due to customer concerns about US spying. Gerry Smith,

largely foundered on partisan bickering.[212] However, there are some encouraging signs of progress, such as the bipartisan passage of the USA Freedom Act to reform the National Security Agency's bulk collection of telephone data.[213] If such high-profile reforms can be successful, then lower-profile consumer reforms are at least possible. Consumers urgently need national laws to help protect them from data breaches, and while those laws are not forthcoming right now, sustained pressure on lawmakers could change that dynamic.

Even if reforms were imminent, businesses would almost certainly oppose any reforms that force them to spend money improving their data security.[214] Complaints from the business community about the cost of regulation are common, although such complaints almost certainly exaggerate true regulatory costs.[215] Government regulation, while undoubtedly not

---

'Snowden Effect' Threatens U.S. Tech Industry's Global Ambitions, HUFFINGTON POST (Jan. 24, 2015), http://www.huffingtonpost.com/ 2014/01/24/edward-snowden-tech-industry_n_4596162.html [http://perma.cc/ F6H6-2HN2]. Snowden was granted political asylum in Russia following his disclosures, with little likelihood of returning to the US without facing dozens of criminal charges. *Edward Snowden: Leaks That Exposed US Spy Programme*, *supra*.

212. *See* Michael Mimoso, *Cybersecurity Legislation Forecast Is Grim*, THREATPOST (Oct. 23, 2014), http://threatpost.com/cybersecurity-legislation-forecast-is-grim/108982 [http://perma.cc/ZE87-GZ98].

213. Erin Kelly, *Senate Approves USA Freedom Act*, USA TODAY (June 2, 2015), http://www.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/ [http://perma.cc/RZ9B-WGPN]. The reform legislation was pushed through the Senate by a coalition of liberal Democrats and libertarian-leaning Republicans seeking to rein in what they saw as an abuse of government surveillance power. *Id.* "Many lawmakers said they were shocked when former NSA contractor Edward Snowden revealed the existence of the NSA's bulk collection program in 2013." *Id.*

214. *See, e.g.*, Letter from Cal. Chamber of Commerce et al. to Roger Dickinson and Bob Wieckowski, Assembly Members, Cal. Gen. Assembly (Apr. 21, 2014), http://www.ctia.org/docs/default-source/Legislative-Activity/coalition-letter-in-opposition-to-california-assembly-bill-1710-regarding-data-management-requirements.pdf?sfvrsn=0 [http://perma.cc/Y9BC-A4NG]. Signed by twenty-one industry trade groups, including the California Chamber of Commerce and the Motion Picture Association of America, the letter opposed amendments to California's existing state privacy laws on a number of grounds, most notably the cost of implementation. *Id.* Despite the opposition, the bill passed and was signed into law in September 2014. Judy Greenwald, *California Law Requires Free Year of Credit Monitoring After Data Breaches*, BUSINESS INS. (Oct. 1, 2014), http://www.businessinsurance.com/article/20141001/NEWS07/141009978 [http://perma.cc/5ER7-LQXY].

215. *Compare* Chad Moutray, *Stop the Insanity: Federal Regulations Cost U.S. Businesses $2 Trillion*, FOX NEWS (Sept. 10, 2014), http://www.foxnews.com/opinion/2014/09/10/study-federal-regulations-cost-us-businesses-2-trillion/ [http://perma.cc/X585-8JZM], *and* Quick Facts, SMALL BUSINESSES FOR SENSIBLE

without expense, does not appear to cause businesses to shed jobs, stop manufacturing their products, or cease serving their customers.[216] Businesses instead adapt and adjust their operations as necessary to comply with regulation, often finding innovative new market opportunities for expansion in the process.[217] Furthermore, with average costs nearing $6 million per data breach,[218] businesses could actually reap significant financial benefits through compliance with statutory reforms that both limit exposure to breaches and decrease their frequency.[219] It should also be noted that if everyone is required to comply, then there would not be any competitive disadvantages to any one business from spending money on new data security measures.

CONCLUSION

Far from being a partisan or controversial issue, robust consumer protection should unite anyone who uses credit cards. With an estimated 183 million American cardholders in

---

REGULATIONS, http://www.sensibleregulations.org/resources/facts-and-figures/ [http://perma.cc/M5L2-ZKF3], *with* Ruth Marcus, *Bad Science Around 'Job-killing Regulations'*, WASH. POST (Apr. 24, 2012), http://www.washingtonpost.com/opinions/bad-science-around-job-killing-regulations/2012/04/24/gIQARQQTfT_story.html [http://perma.cc/38HA-2TPW].

216. Marcus, *supra* note 215; *see also* Jeff Spross, *Why EPA's Carbon Regulations Won't Ruin the Economy, in Three Simple Steps*, THINKPROGRESS (June 3, 2014), http://thinkprogress.org/climate/2014/06/03/3444064/epa-explainer-economy/ [http://perma.cc/AAQ2-4VKZ]; *see also* ISAAC SHAPIRO & JOHN IRONS, ECONOMIC POLICY INSTITUTE, REGULATION, EMPLOYMENT, AND THE ECONOMY: FEAR OF JOB LOSSES ARE OVERBLOWN (2011), http://www.epi.org/publication/regulation_employment_and_the_economy_fears_of_job_loss_are_overblown/ [http://perma.cc/PA2K-663T].

217. *E.g.*, CDP NORTH AMERICA, THE BUSINESS RESPONSE TO CLIMATE CHANGE ACROSS AMERICA (2014), https://www.cdp.net/CDPResults/CDP-state-by-state-report-2014.pdf [https://perma.cc/33HA-753E] (concluding that companies are innovating in response to expected climate change management regulation).

218. PONEMON INST., *supra* note 90.

219. *See, e.g.*, Amitai Etzioni, *Cybersecurity in the Private Sector*, 28 ISSUES IN SCI. AND TECH. 1 (2011), http://issues.org/28-1/etzioni-2/ [http://perma.cc/LUK4-ZTRD] (discussing cybersecurity incentives in private and public sector organizations). *But see* Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity*, CONVERSATION (Mar. 4, 2015), http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570 [http://perma.cc/JT4T-K7NY] (arguing that businesses have little real incentive to invest in cybersecurity due to the low relative cost of dealing with data breaches compared to overall sales revenue).

2011,[220] there is no doubt that the pool of potential data breach victims spans across the political and economic spectrum. Because of the highly distributed nature of data breaches in our electronic exchange economy, consumer rights and remedies under current common, statutory and regulatory law are clearly inadequate. However, there are steps that can be taken to enhance consumer rights and remedies. By adopting an improved definition of personally identifiable data, creating a new definition of data controllers and processors, and reforming statutory liability for data breaches, Americans can be protected, and protect themselves, from the serious risks posed by consumer data breaches both now and in the future. Data breaches are only going to become more common, so these steps should be taken as soon as possible. Otherwise, the toll data breaches incur on our economy will only grow with time.

220. U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES: 2011, at 740 (2011).