DATA BREACHES, BITCOIN, AND BLOCKCHAIN TECHNOLOGY: A MODERN APPROACH TO THE DATA-SECURITY CRISIS

Stephen Jones[*]

---

* J.D. Candidate, Texas Tech University School of Law, May 2019; B.A. Communications, Colorado State University, 2015. This Comment is dedicated to the memory of a dear friend, mentor, and Texas legal legend: Professor John E. Krahmer. To my friend Bobby "Base" Sharp, thank you for your inspiration and guidance in helping me shape the overall vision for this Comment. To all of my family and friends, thank you for always encouraging me to pursue my dreams—I would not be the man I am today without your support.

I. ANOTHER DAY, ANOTHER DATA BREACH: WELCOME TO THE TWENTY-FIRST CENTURY EPIDEMIC

On September 7, 2017, Equifax issued startling news: 143 million Americans were exposed to the future risk of identity fraud after the company experienced a significant data breach.[1] Texas resident Stephen Luce was one of the many people affected by the incident.[2] After news of the breach broke, Luce visited Equifax's website to determine whether he was one of the unlucky persons whose information was at risk; his fear was confirmed.[3] Shortly after confirming his information had been leaked, Luce received notices from two credit card companies with whom he held accounts, informing him that attempts had been made to change his address, phone numbers, and email contact information.[4] The fraudulent individuals succeeded in changing Luce's personal information, and since then, he has had to deal with reclaiming his accounts and the continuing fear of future

1. Jobin Panicker, *Equifax Breach 'On Different Scale'*, WFFA (Sept. 19, 2017, 2:04 PM), http://www.wfaa.com/mobile/article/news/crime/equifax-breach-on-different-scale/477005334?scroll=797; *see* Geoff Williams, *What Is Equifax and Why Does It Have My Financial Information?*, U.S. NEWS & WORLD REP. (Sept. 19, 2017, 10:03 AM), https://money.usnews.com/money/personal-finance/banking-and-credit/articles/2017-09-19/what-is-equifax-and-why-does-it-have-my-financial-information (explaining that Equifax is a credit-reporting agency that compiles consumer information into a credit report for use by lenders in assessing a consumer's financial viability).

2. Panicker, *supra* note 1.

3. *Id.*

4. *Id.*

fraudulent activity.[5] Unfortunately, because the scope of the breach is one of unprecedented proportions, stories like Luce's will likely become common.[6]

The United States has experienced data breaches in the past, but what makes the Equifax situation so unique and concerning to consumers is the *type* of information that has now been compromised.[7] The Equifax "hackers seized names, Social Security numbers, birth dates, addresses and even some driver's license information."[8] Furthermore, the response from Equifax in the wake of the breach has been far from comforting to those affected.[9] Equifax initially offered complimentary credit monitoring to victims who sought its assistance but required the victims to agree to mandatory arbitration and waive their right to join any class-action suit.[10] The company has since disavowed the arbitration agreement.[11] Nonetheless, the company requires victims to send a notice of their intent to opt out of the arbitration agreement within thirty days of signing up for the monitoring service.[12] Additionally, legal experts predict that Equifax could convincingly argue that the binding arbitration clause does, in fact, limit consumers in their remedies.[13]

With the number of data-breach incidents rising and remedies for consumers being minimal at best, the time has come for the United States to take a hard look at current data-breach regulations and implement policies, practices, and guidelines that are fitting for a twenty-first century society.[14] Solutions to data security, such as implementing the use of "blockchain" technology, are becoming prevalent in how data is stored, protected, and verified; some countries have adopted such practices at a nation-wide

---

5. *Id.*

6. *See id.*

7. Nathan Bomey et al., *Equifax Data Breach: What You Need to Know about Hacking Crisis*, USA TODAY (Sept. 18, 2017, 12:19 PM), https://www.usatoday.com/story/money/2017/09/15/equifax-data-breach-what-you-need-know-hacking-crisis/670166001/.

8. *Id.*

9. *See* Michelle Mark, *Signing Up for Equifax's Help Site Could Mean You're Waiving Your Right to a Class-Action Lawsuit*, BUS. INSIDER (Sept. 8, 2017, 2:36 PM), http://www.businessinsider.com/equifax-help-site-mandatory-arbitration-clause-waive-right-to-class-action-lawsuit-2017-9.

10. *See id.*

11. *See id.*

12. *See id.*

13. *See id.* "'If you just look at the terms of the arbitration agreement, there's an argument that it would cover the underlying data breach,' Leah Nicholls, a staff attorney at the nonprofit law firm Public Justice, told Business Insider." *Id.* "If Equifax is serious about this arbitration agreement not applying to its underlying data breach, it should rewrite its arbitration agreement or get rid of it." *Id.*

14. *See* Elizabeth Weise, *Equifax Breach: Is It the Biggest Data Breach?*, USA TODAY (Sept. 7, 2017, 7:35 PM), https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/ (comparing the Equifax breach with other recent data breaches that have occurred in the United States); Kaya Yurieff, *Why Are We Still Using Social Security Numbers as ID?*, CNN (Sept. 13, 2017, 8:40 AM), http://money.cnn.com/2017/09/13/technology/social-security-number-identification/ index.html (suggesting that "[t]he [Social Security] number can stay, but we shouldn't rely on it to prove who you are . . . . You should just assume anybody could have that number").

level.[15] Estonia, a small European country, now allows citizens to vote, maintain health records, pay taxes, make transactions, register childbirths, and perform countless other tasks, all using a computer; blockchain technology and proactive data-protection procedures are the driving forces of its system.[16] With suitable alternatives available and technology being increasingly adopted into American culture, now is the time for a complete system overhaul.[17]

This Comment explores what data breaches are and how their prevalence has steadily increased in American society; federal and state law on data-breach and data-protection issues and the shortcomings of the current regulation scheme; and the legal burden on consumers and businesses in the aftermath of a breach. This Comment then examines the new and emerging world of blockchain technology and the variety of ways it is being used to securely transfer and store data. Finally, a recommendation is posed involving a series of steps that should be taken to revamp our current governmental system with both legal and technological solutions that could mitigate and prevent future data-breach issues. Part II of this Comment provides a general overview of data breaches and their widespread consequences.[18] Part III outlines federal and state law, as well as United States Supreme Court precedent that relates to data breaches and makes clear why the current system is ineffective.[19] Part IV introduces blockchain technology and explains why many believe that it will fundamentally change the way society functions.[20] Finally, Part V ties together how data-breach legal reform and blockchain technology are related to the central concept of data security and data protection and provides guidance on how government officials should address the data-breach epidemic.[21]

II. TECHNOLOGICAL DILEMMA: DATA BREACHES EXPLAINED

The Identity Theft Resource Center (ITRC) "defines a data breach as an incident in which an individual name plus a Social Security number, [d]river's [l]icense number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure."[22] Hackers can

15. Vivienne Walt, *Is This Tiny European Nation a Preview of Our Tech Future?*, FORTUNE (Apr. 27, 2017, 9:08 AM), http://fortune.com/2017/04/27/estonia-digital-life-tech-startups/.

16. *See id.*

17. *See id.*; Aaron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, PEW RES. CTR. (Jan. 12, 2017), http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/ (showing that a significant portion of Americans now own smartphones and tablet computers, have access to home broadband internet, and use social media regularly).

18. *See infra* Part II.

19. *See infra* Part III.

20. *See infra* Part IV.

21. *See infra* Part V.

22. *Data Breaches: Overview*, IDENTITY THEFT RES. CTR. (Sept. 21, 2017), http://www.idtheftcenter.org/Data-Breaches/data-breaches [hereinafter *Data Breaches: Overview*].

achieve a successful breach in a variety of ways, but they typically carry them out "by accessing a computer or network to steal local files, or by bypassing network security remotely."[23] Hackers spend time planning their infiltration, and once they have successfully gained access to a network, they can extract information from virtually all data held in that network.[24]

From 2005 to the end of 2017, there were 8,190 data breaches in the United States resulting in the exposure of an estimated 1,057,771,011 records.[25] To put the regularity of their occurrences into perspective, since beginning research on this Comment in the fall of 2017, the number of exposed records has increased by over 150 million.[26] The United States has fallen victim to much larger data breaches than the recent Equifax breach.[27] The largest to date was the Yahoo data breach in 2016, when the company announced that an estimated one billion of its users' confidential account information had been exposed.[28] Yahoo is now facing significant class-action suits after, in a somewhat rare occurrence, a California judge upheld standing for the plaintiffs, concluding that "all Plaintiffs have alleged a risk of future identity theft, in addition to loss of value of their [personal identification information]."[29] Although the Yahoo breach was large in its numbers, the Equifax data breach adds a startling new twist to the data-breach epidemic.[30]

A. An Unfamiliar Ailment: Equifax and Its Aftermath

The Equifax breach is unique in its consequences for consumers.[31] What distinguishes the Equifax breach is that individuals do not create accounts with Equifax or expressly grant the company access to their personal information.[32] Instead, Equifax acts as a credit-reporting agency and collects consumer information based on credit transactions and

---

23. *Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes*, TREND MICRO (Oct. 23, 2015), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

24. *See id.*

25. *Data Breaches: Overview*, *supra* note 22.

26. *See id.* From September 7, 2017 to December 27, 2017, the number of exposed records has increased from 907,293,703 to 1,057,771,011. *Id.*

27. *See* Weise, *supra* note 14. The Yahoo breach in 2016 affected one billion users, the MySpace breach in 2016 affected 350 million users, and the eBay breach in 2014 affected 145 million users. *Id.*

28. *See id.*

29. *See In re* Yahoo! Inc. Customer Data Sec. Breach Litigation, No. 16-MD-02752-LHK, 2017 WL 3727318, at *17 (N.D. Cal. Aug. 30, 2017); Jonathan Stempel, *Yahoo Must Face Litigation by Data Breach Victims: U.S. Judge*, REUTERS (Aug. 31, 2017, 10:12 AM), https://www.reuters.com/article/us-verizon-yahoo-breach/yahoo-must-face-litigation-by-data-breach-victims-u-s-judge-idUSKCN1BB25Q. The California court's holding was somewhat rare because courts are split on what will satisfy standing in data-breach suits. *See infra* Part III.B (analyzing the difficulty of proving standing in data-breach litigation).

30. *See* Bomey et al., *supra* note 7; Weise, *supra* note 14.

31. *See* Bomey et al., *supra* note 7.

32. *See* Williams, *supra* note 1.

repayment history.[33] That information is then used to generate a credit report.[34] Credit-reporting agencies then sell the reports "to banks, credit unions, insurance firms, retailers, utilities and government agencies—generally any company or organization that is involved in your financial life."[35] Consumers have minimal control over how the information is collected, protected, and, more importantly, who may receive it.[36] However, companies like Equifax do serve a valuable purpose in helping consumers show their track record for repayment of outstanding debt and their ability to repay future debt.[37] The problem is that once a consumer's personal information is leaked, "[it is] hard to stop [hackers] from trying to prove that they are [the consumer]."[38] Experts contend that the only way for a consumer to fully protect their identity from fraudulent use "require[s] a new [S]ocial [S]ecurity number, which is close to impossible."[39]

B. Countless Victims: Data-Breach Repercussions

Data-breach occurrences affect the consumers whose records are exposed as well as the companies who leak the information.[40] Consumers incur "increased risk of identity theft or fraud and, more recently, 'sorting-things-out' costs and [identity] monitoring expenditures."[41] The risk

---

33. *See id.*

34. *See id.*

35. *Id.*

36. *See id.*; *see* Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 46 (2015) ("Because captured personal information is collected during an initial transaction and often subsequently transferred to another business or sold for profit, the traceability of personal information is reduced, making it nearly impossible for individuals to monitor the privacy and security of their personal information.").

37. *See* Williams, *supra* note 1.

38. *Id.*

39. *Id.*

40. Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017) (discussing the ramifications of data breaches on consumers and businesses); Toni Forder, *5 Unbelievable Data Leak Horror Stories and Why You Should Amp Your Data Security Today*, TRANSCOSMOS INFO. SYS. (Oct. 1, 2015), http://transcosmos.co.uk/blog/5-unbelievable-data-leak-horror-stories-and-why-you-should-amp-your-data-security-today/ (listing large cyber-attacks and warning businesses to take preventative measures before data breaches occur).

41. Dowty, *supra* note 40.

> The costs associated with sorting things out are distinct from the purchase of monitoring services and generally encompass less easily calculable expenses, such as personal time expended canceling cards and ordering new ones, changing passwords or pin numbers, calling companies directly to verify suspicious communications received from them, closing banking accounts and opening new ones (if the bank account number was exposed), having a credit reporting agency place a fraud alert on one's account (if one's social security number was exposed), placing a credit freeze on one's account, inserting new card information into one's auto-fill program, changing recurring payment methods, and communicating with banks.

Id.

of information exposure to the millennial generation is especially problematic because many in that group are coming to an age of which purchases of homes, cars, and other valuable assets require an inquiry into credit scores.[42] Furthermore, because many in the millennial age bracket have short credit histories, the effects of fraudulent activity can have a significant impact on their ability to receive loans and prove credit history, and it can take long periods of time to reverse any damage that has been done.[43]

The companies who leak consumer information also face significant financial harm, as evidenced by Target's recent data leak, which could amount to $3.6 billion in company expenses.[44] Analysts suggest that "small businesses are even more unprepared for a cyber-breach than larger corporations, partly because they falsely believe [that] they are too tiny to target, thus automatically dropping beneath the cyber crooks' radar . . . ."[45] Regardless of size, IBM reports that the average cost to businesses per leaked record is $141.[46] The cost to the global economy resulting from data breaches is predicted to reach $2 trillion by 2019, and North American countries are picking up the brunt of the bill.[47] To better understand the identity-fraud risk faced by consumers after a breach occurs, the following section will survey commonly-used forms of identification focusing on those that are most prone to fraudulent use.

C. Contaminated Identity: The Information Hackers Pursue

United States citizens utilize a variety of ways to prove identity.[48] The current methods used are often purpose-specific (for example, seeking employment), and typically must be used in conjunction with one another to

---

42. *See* Danielle Wiener-Bronner, *Why Millennials Should Be Really Worried about the Equifax Breach*, CNN MONEY (Sept. 15, 2017, 4:21 PM), http://money.cnn.com/2017/09/15/pf/millennials-equifax-breach/index.html?iid=EL (arguing that millennials are at a heightened risk for credit harm when their information is used fraudulently).

43. *See id.*; Richard Fry, *Millennials Projected to Overtake Baby Boomers as America's Largest Generation*, PEW RES. CTR. (Apr. 25, 2016), http://www.pewresearch.org/fact-tank/2016/04/25/millennials-overtake-baby-boomers/ (explaining that the millennial generation is now the largest living generation and the group includes those born from 1981 to 1996).

44. *See* Forder, *supra* note 40.

45. Dimitar Kostadinov, *How Harmful Can a Data Breach Be?*, INFOSEC INST. (Sept. 30, 2015), http://resources.infosecinstitute.com/the-cost-of-a-data-breach-how-harmful-can-a-data-breach-be/#gref.

46. *See 2017 Ponemon Cost of Data Breach Study*, IBM SEC., https://www.ibm.com/security/data-breach/ (last visited Mar. 28, 2018).

47. *See* Zack Wittaker, *Data Breaches to Cost Global Economy $2 Trillion by 2019*, ZD NET (May 12, 2015, 8:23 PM), http://www.zdnet.com/article/data-breaches-to-cost-2-trillion-by-2019/ (arguing that the global economy suffers from the acts of "cyber criminals because of poor corporate and network security").

48. *See, e.g.*, *Acceptable Identification Documents*, TEX. DEP'T OF PUB. SAFETY (Aug. 2016), https://www.dps.texas.gov/internetforms/Forms/DL-17.pdf (listing accepted forms of identification in Texas as: state-issued driver's license, Social Security Card, birth certificate, Voter Registration Card, U.S. Passport, American Indian Card, etc.).

prevent identity fraud.[49] Many argue that an individual's Social Security number is the most sensitive piece of personal information that can be exposed in a data breach.[50] At its inception, the Social Security program and accompanying card were designed to track American wage histories and "for use in determining Social Security benefit entitlement and computing benefit levels."[51] Experts have long criticized the use of Social Security cards to verify identity and have warned of their potential risk for identity fraud.[52] Experts argue that "Social Security numbers were never intended to verify a person is who he says he is . . . ."[53] Replacement cards can be issued in the event of a lost or stolen card, but changing one's Social Security number can only be done under very limited circumstances.[54] Though identity theft is listed as one of the circumstances for obtaining a new number, the identity-theft victim is required to show a continuous disadvantage in keeping their current number, and the factors for assessing what meets the standard are unclear.[55]

Another form of commonly carried self-identification that is highly susceptible to fraudulent use is a state-issued driver's license.[56] For instance, in Texas, if a person is the victim of identity theft due to a data breach, the

---

49. *See Proof of U.S. Citizenship and Identification When Applying for a Job*, U.S. CITIZENSHIP AND IMMIGR. SERV. (Feb. 3, 2010), https://www.uscis.gov/us-citizenship/proof-us-citizenship-and-identification-when-applying-job (detailing different forms of identification and how they can be used to prove citizenship and the right to work in the United States).

50. *See* Bill Fay, *Identity Theft*, DEBT.ORG, https://www.debt.org/credit/identity-theft/ (last visited Mar. 28, 2018) (opining that one's Social Security number "might be the most valuable information you have to protect"); *9 Most Common Types of Identity Theft*, MOUNTAIN ALARM FIRE & SEC. (June 14, 2016) [hereinafter *Types of Identity Theft*], https://www.mountainalarm.com/blog/9-most-common-types-of-identity-theft/ (providing ways a Social Security number can be fraudulently used, including: the purchase and use of the number by undocumented workers to gain employment, and the forging of documents to open credit card accounts and obtain government documents such as a passport).

51. Carolyn Puckett, *The Story of the Social Security Number*, SOC. SECURITY ADMIN. (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html (analyzing the history of the Social Security system and the corresponding card).

52. *See* Tamara Chuang, *Why Does Your Identity Depend on One Number? Security Experts Push to Replace SSN*, DENVER POST (Sept. 15, 2017, 5:16 PM), http://www.denverpost.com/2017/09/15/equifax-data-breach-social-security-number-replacement/ (criticizing the continued reliance on Social Security cards as a form of identification).

53. *Id.*

54. *See Frequently Asked Questions – Can I Change My Social Security Number?*, SOC. SECURITY ADMIN., https://faq.ssa.gov/link/portal/34011/34019/article/3789/can-i-change-my-social-security-number (last visited Mar. 28, 2018) ("We can assign a different number only if: [s]equential numbers assigned to members of the same family are causing problems; [m]ore than one person is assigned or using the same number; [*a*] *victim of identity theft continues to be disadvantaged by using the original number* . . . ." (emphasis added)).

55. *See id.* (explaining that obtaining a new Social Security card or number in the event of identity fraud can be placed into the category of "costs of sorting things out"). The Social Security Administration does not provide an explanation of the factors it considers when assessing whether to issue a new Social Security number. *See id.*; *see also* Dowty, *supra* note 40, at 709 (defining "costs of sorting things out").

56. *See Types of Identity Theft*, *supra* note 50 (warning consumers that "in most instances, criminals use [stolen] driver's license [information] to hide or protect their own identity if they are caught in compromising or dangerous situations").

state requires the victim to first file a police report.[57] The Texas Department of Public Safety then has discretion whether to issue a new license or deny the application and, similar to a Social Security card, the factors the department uses to determine whether to issue a new driver's license number are unclear.[58]

Lastly, most American-born citizens possess a birth certificate.[59] Individuals can acquire replacement copies of birth certificates from state offices, but because one does not pick a date of birth or have the ability to change it, a person's birthdate is especially vulnerable if it is compromised in a data breach.[60] In addition to financial costs and the increased risk of identity fraud, data breaches present legal ramifications for all involved parties—the following Part outlines the complicated framework of data-breach law.

III. THE EPIDEMIC COMPOUNDED: UNITED STATES LAW ON DATA-BREACH ISSUES

As of the time of this Comment's publication, the United States does not have a statute enacted covering uniform data-breach notification to consumers or general data-protection standards for businesses that collect personal information.[61] Current federal legislation is industry-specific and often leaves data-breach victims without a cause of action, as evidenced by the fact that many courts have held that consumers lack standing to bring suit.[62] Conversely, "[f]orty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands" have enacted data-protection and data-breach notification laws, few of which provide consumers with a private cause of action.[63] Companies who fall victim to a cyber attack and do

---

57. *See How to Replace Your Driver License or ID Card*, TEX. DEP'T OF PUB. SAFETY, https://www.dps.texas.gov/DriverLicense/replace.htm (last visited Mar. 28, 2018) (leaving unaddressed the specific circumstances that permit issuance of a new driver's license after identity fraud occurs).

58. *See id.* (obtaining a new driver's license or number can be put into the category of "costs of sorting things out"). The Texas Department of Public Safety is vague in its explanation of what circumstances warrant the issuance of a new driver's license number. *See id.*; Dowty, *supra* note 40, at 689 (referencing the costs of sorting things out).

59. *See How to Apply for Birth Certificate and Other Vital Documents for Newborn in US?*, PATH2USA, https://www.path2usa.com/how-to-apply-for-birth-certificate (last visited Mar. 28, 2018).

60. *See Replace Your Vital Records*, USA.GOV (Oct. 2, 2017), https://www.usa.gov/replace-vital-documents.

61. *See* Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1174–75 (2014) (outlining the dilemma of statutory confliction and shortage of industry coverage in current federal data-breach regulations).

62. *See id.*

63. *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Feb. 6, 2018) [hereinafter *Security Breach*], http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Alabama and South Dakota do not have data-breach notification laws. *Id.* Alaska, California, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, Washington, District of Columbia, Puerto Rico, and the Virgin Islands allow for private causes of action. *Id.*

business across the nation are expected to comply with the data-related statutes for each state in which they do business.[64] The intertwining and unclear scheme of data-breach regulations, and the issues consumers face in proving standing to bring suit, makes compliance for companies burdensome and presents difficulty to consumers in seeking relief.[65]

A. Defects in the System: The Limited Scope of Federal Regulations

Federal data-breach statutes apply almost exclusively to specific industries.[66] The industries include banking, finance, healthcare, and credit reporting.[67] These statutes leave open the specific issue of "data-breach notification for consumers."[68] Those affected by the Equifax breach will likely seek a cause of action under the Fair Credit Reporting Act (FCRA), which limits sharing of consumer credit information by credit-reporting agencies to expressly authorized purposes.[69] The FCRA also mandates that credit-reporting agencies implement reasonable procedures to protect consumer information from prohibited disclosure.[70] However, the statute fails to provide examples of reasonable procedures or explain how businesses can assess their vulnerability for future data breaches.[71] Further, the statute mandates that if the credit-reporting agency is found to be in "willful noncompliance" with procedural requirements, remedies are limited to actual damages sustained by the consumer but courts may assess punitive

---

64. *See generally id.*

65. *See* Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, NOTRE DAME L. REV. 1323, 1326 (2017) (illustrating the inconsistency in federal courts of what satisfies standing requirements in data-breach litigation); Peters, *supra* note 61.

66. *See* Peters, *supra* note 61, at 1176. Data-breach statutes include:

> (1) the Computer Fraud and Abuse Act ("CFAA"); (2) the Electronic Communications Privacy Act ("ECPA"); (3) healthcare privacy laws, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); and (4) financial data laws including the Gramm-Leach-Bliley Act of 1999 ("GLBA") and Red Flags Rules of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). Other federal laws include the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the Fair Credit Reporting Act, the Bank Secrecy Act, and the Children's Online Privacy Protection Act.

Id. (internal quotations omitted).

67. *See id.* at 1174–76.

68. *See id.* at 1178.

69. *See* 15 U.S.C.A. § 1681b(f)(1) (2018) (making clear that "A person shall not use or obtain a consumer report for any purpose unless—(1) the consumer report is obtained for a purpose for which the consumer report is authorized to be furnished under this section; and (2) the purpose is certified in accordance with section 1681e of this title by a prospective user of the report through a general or specific certification"). Consumers could potentially have a cause of action under the Gramm-Leach-Bliley Act but because the Act is limited in scope to financial institutions, recovery under the statute will be unlikely. *See* Peters, *supra* note 61, at 1180.

70. 15 U.S.C.A. § 1681e(a) ("Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations . . . .").

71. *See id.*

damages.[72] Though the statute attempts to make companies responsible for their failure to protect consumer information, many class-action suits result in a substantial underpayment of the mandated damages because companies often settle the disputes out of court.[73] As a result, the small settlements leave consumers substantially undercompensated and responsible for any future damage they may incur.[74]

Because of the significant uptick in data-breach occurrences and the widespread effect on American citizens, there has been a renewed push for uniform federal legislation.[75] Lawmakers in Washington have taken notice of the lack of coverage in federal data-breach legislation and have started to propose bills addressing the problem.[76] The bills vary in approach.[77] For example, the Data Breach Prevention and Compensation Act of 2018 suggests the creation of a Cybersecurity Office that would be part of the Federal Trade Commission (FTC).[78] The proposal would require the Cybersecurity Office to impose regulations and data-protection procedures on consumer-reporting agencies.[79] The proposal would impose penalties on

---

72. *Id.* § 1681n(a).

> Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of—(1)(A) any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000; or (B) in the case of liability of a natural person for obtaining a consumer report under false pretenses or knowingly without a permissible purpose, actual damages sustained by the consumer as a result of the failure or $1,000, whichever is greater; (2) such amount of punitive damages as the court may allow; and (3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

Id.

73. *See* Ian Salisbury, *Wanna Sue Equifax? Here Are All Your Options*, TIME MONEY (Sept. 22, 2017), http://time.com/money/4949869/equifax-data-breach-lawsuits/ (explaining how "retail giant Target agreed to pay $18.5 million after hackers [sic] stole personal information from up to 40 million credit and debit cards," resulting in a payment of approximately $0.50 per affected customer).

74. *See* Dowty, *supra* note 40, at 713.

75. *See* Patrick Howell O'Neill, *National Data Breach Notification Law Proposed by Senate Commerce Committee Members*, CYBERSCOOP (Nov. 30, 2017), https://www.cyberscoop.com/national-data-breach-notification-law-bill-nelson-uber-equifax-hack/ (reporting on proposed legislation that would issue harsh penalties for businesses that fail to protect consumer information).

76. *See* Data Breach Prevention and Compensation Act of 2018, S. 2289, 115th Cong. (2018) ("To create an Office of Cybersecurity at the Federal Trade Commission for supervision of data security at consumer reporting agencies, to require the promulgation of regulations establishing standards for effective cybersecurity at consumer reporting agencies, to impose penalties on credit reporting agencies for cybersecurity breaches that put sensitive consumer data at risk, and for other purposes."); Consumer Privacy Protection Act of 2017, S. 2124, 115th Cong. (2017) ("To ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information."); Data Security and Breach Notification Act, S. 2179, 115th Cong. (2017) ("To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.").

77. *See* S. 2289; S. 2124; S. 2179.

78. *See* S. 2289.

79. *See id.*

companies that fail to protect consumer information, but noticeably absent is an express private cause of action for consumers.[80] Two other approaches, the Consumer Privacy Protection Act of 2017 and the Data Security Breach Notification Act, would also require the FTC to create data-protection regulations.[81] Additionally, the two bills seek to have credit-reporting agencies implement preventative data-breach measures and provide timely notice to consumers if a data breach does occur.[82] Like the first bill, neither proposal grants an express private cause of action for consumers, but they do impose civil penalties for violations.[83] To encourage businesses to comply, both proposals mandate that any person who willfully and intentionally conceals a data breach will face monetary penalties and a possible term of imprisonment for up to five years.[84] Although it will likely take time for the bills to make their way through the legislative process, the legislature has taken positive steps toward solving the problem by recognizing data-breach regulation deficiencies and by initiating discussions to enact uniform legislation.

B. Further Breakdown: The Standing Problem in Data-Breach Litigation

Even if consumers allege a statutory violation under applicable federal law, they face another challenge in seeking relief. The challenge arises from Supreme Court precedent and the differences in how lower federal courts have interpreted what satisfies the injury requirement for standing.[85] The major difficulty for data-breach plaintiffs is proving that they have a "sufficient injury in fact that is 'concrete and particularized' and 'actual or imminent,' not 'conjectural' or 'hypothetical.'"[86] The United States Supreme Court has held what many believe to be conflicting positions on what satisfies the requirement.[87] The Court's perceived inconsistency has resulted in a

---

80. *See id.*
81. *See* S. 2124; S. 2179.
82. *See id.*
83. *See id.*
84. *See id.*
85. *See generally* Mank, *supra* note 65.
86. *See id.* at 1330. The test requires:

> [A] plaintiff to show that: (1) she has 'suffered an injury in fact,' which is (a) 'concrete and particularized' and (b) 'actual or imminent, not "conjectural" or "hypothetical"'; (2) 'there [is] a causal connection between the injury and the conduct complained of—the injury has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result[] [of] the independent action of some third party not before the court"'; and (3) "it [is] "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision."'

Id. (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

87. *See* Clapper v. Amnesty Int'l USA, 113 S. Ct. 1138, 1141 (2013) (suggesting a high burden of proof to meet the "certainly impeding" harm requirement); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–50 (2016) (holding that though the plaintiff alleged a federal statutory violation by the defendant, a concrete injury must also be shown); Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (holding that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly

stark split in the federal circuits, which in turn makes recovery for plaintiffs uncertain.[88] The uncertainty centers on the question of whether the mere disclosure of personal information is enough to bring suit, or whether the information must also be fraudulently used, establishing injury.[89]

The U.S. District Court for the Southern District of California upheld standing for data-breach victims in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*.[90] Consumers brought suit against Sony after hackers were able to penetrate the Sony Gaming Network and access personal information including names, credit cards, and other payment information.[91] The district court applied a "credible threat" test and found that the plaintiffs satisfied standing because they presented evidence that their information was at risk due to Sony's failure to protect the data.[92]

The U.S. District Court for the Northern District of Illinois came to a similar conclusion in *Moyers v. Michaels Stores, Inc.*[93] In that case, a group of plaintiffs sued Michaels after malicious hacker software embedded in the company's system compromised consumer credit-card information.[94] The court relied on evidence presented by *one* plaintiff whose credit card was used fraudulently two weeks after the breach, to uphold standing for *all* plaintiffs recognizing an increased risk of future harm.[95]

Conversely, the U.S. District Court for the District of Columbia denied standing to plaintiffs in *In re Science Application International Corp. Backup Tape Data Theft Litigation*.[96] The suit involved stolen data disks that contained the personal information of 4.7 million members of the United States military.[97] The court held that the individuals whose information had actually been used fraudulently could move forward with their claims, but those whose information had only been put at risk were precluded from seeking relief.[98] Similarly, in *Hammond v. Bank of New York Mellon Corp.*, the U.S. District Court for the Southern District of New York denied standing to plaintiffs whose information had been compromised.[99] The plaintiffs

---

impending,' or there is a 'substantial risk' that the harm will occur").

88. *See generally* Mank, *supra* note 65 (implying that a plaintiff's recovery depends largely on how the court interprets what will satisfy standing).

89. *See id.* at 1325–27.

90. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014), *order corrected by*, MDL No.11md2258 AJD (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

91. *Id.* at 955.

92. *Id.* at 962.

93. Moyers v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014).

94. *Id.* at *1–2.

95. *Id.* at *2–6.

96. *In re* Science Application Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 24–28 (D.D.C. 2014).

97. *Id.* at 19.

98. *Id.* at 26–34.

99. *See* Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307

alleged that the defendant failed to protect their information after records were lost during transportation and data was leaked after a security breach.[100] The court found that the plaintiffs "lack[ed] standing because their claims [were] future-oriented, hypothetical, and conjectural."[101]

Federal courts' differing interpretations of what satisfies standing further complicates and underscores the uncertainty plaintiffs face when seeking relief.[102] Looking to the Equifax breach, attorneys across the country have filed as many as fifty class-action suits against Equifax, including one that encompasses plaintiffs from all fifty states and the District of Columbia.[103] Counsel representing the plaintiffs in the fifty-state class-action alleges that, "[c]riminals are using the stolen information to apply for mortgages, credit cards and student loans, and tapping into bank debit accounts, filing insurance claims and racking up substantial debts . . . ."[104] The allegations will likely meet the standing requirement for those who can prove actual fraudulent use of their information, however, those who cannot show fraudulent use may be precluded from seeking relief.[105] However, only time will tell whether lower courts will impose significant penalties on Equifax, and more importantly, whether the Equifax breach will serve as a wake-up call to other companies that are lax in their data-protection measures.

C. Additional Complications: Data-Breach Law at the State Level

State law on data-breach issues differs based on jurisdiction.[106] The forty-eight states that have enacted data-breach related statutes typically share one characteristic: "most require consumer notification only when the compromised data was not encrypted, or when the encryption key was also compromised."[107] The main difference in the statutes is the way the states define "personal information;" some states define it broadly, while other states are more restrictive.[108] Some state laws require companies that collect

---

(S.D.N.Y. June 25, 2010).

100. *Id.* at *2.

101. *Id.* at *7.

102. *See generally supra* Section III.B (explaining the complications involving standing in these cases).

103. *See* Salisbury, *supra* note 73 (reporting on the nationwide class-action suit).

104. *See* Kenneth R. Harney, *Data Breach at Equifax Prompts a National Class-Action Suit*, WASH. POST (Nov. 22, 2017), https://www.washingtonpost.com/realestate/data-breach-at-equifax-prompts-a-national-class-action-suit/2017/11/20/28654778-ce19-11e7-a1a3-0d1e45a6de3d_story.html?utm_term=.aca58d7d6477.

105. *See* Mank, *supra* note 65, at 1330.

106. *See* Peters, *supra* note 61, at 1182.

107. *Id*.

108. *See id.*

> Typically, personal information includes: (a) [a] first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not encrypted, redacted or secured by any other method rendering the element unreadable or

a consumer's personal information to implement reasonable procedures to protect the information, while others leave the issue open.[109] Like federal statutes that have similar requirements, state laws do not guide businesses on what reasonable procedures are, or how businesses can assess their risk of incurring future data breaches.[110] Additionally, many state statutes do not provide consumers with an express cause of action against companies that fail to protect their personal information.[111] The statutes also differ by providing inconsistent ranges-of-time for businesses to notify consumers of a breach, and some allow businesses to first conduct an "analysis of a breach's risk-of-harm as a prerequisite for determining whether notification is required."[112] The following Sections will review the Texas, Nevada, and New York statutes relevant to data-breach notification and data protection, showing the differing approaches states have taken to address the data-breach issue.

1. Southern Style: The Texas Approach

In Texas, the applicable statute is the Identity Theft Enforcement and Protection Act (ITEPA).[113] The ITEPA imposes a duty on data-collecting businesses to "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."[114] In the event of a breach, the ITEPA requires a data-breach notice to be sent to consumers "as quickly as possible." It also allows for businesses to defer to their own information-security policies that differ from the statute's consumer-notification requirements.[115] The ITEPA provides consumers with a cause of action for data-breach harm through the tie-in provision of the Texas Deceptive Trade Practices Act (DTPA).[116] If a data-breach victim is successful in his claim under the DTPA, a court may award attorney's fees

---

> unusable: (i) [a] social security number; (ii) a number on a driver license number . . . or number on a nonoperating identification license number; (iii) [a] financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual's financial account.

Id.

109. *See Data Breach Charts*, BAKERHOLSTER (Nov. 2017), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf (summarizing state statutes on data-breach notification and data protection).

110. *See id.*

111. *See id.*

112. Peters, *supra* note 61, at 1183; *see Security Breach*, *supra* note 63.

113. TEX. BUS. & COM. CODE ANN. § 521.001 (West 2017).

114. *Id.* § 521.052(a).

115. *See id.* § 521.053(b), (g).

116. *See id.* § 521.152.

and up to three times the actual damages incurred by the victim.[117] The ITEPA also provides for a civil penalty paid to the state and permits criminal charges against those who later use the information fraudulently.[118] The statute's remedies to consumers are encouraging, but the vague "reasonable procedures" language provides little guidance to businesses for best prevention practices.[119]

2. Data in the Desert: The Nevada Approach

The applicable statute in Nevada is found under Trade Regulations and Practices.[120] Similar to Texas, the statute provides that businesses that collect consumer data "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."[121] The statute does not clarify what reasonable security measures are, or how businesses should mitigate and prevent future data breaches.[122] The statute does not provide a time requirement for businesses to notify consumers of a breach, and instead states that, "[t]he disclosure must be made in the most expedient time possible and without unreasonable delay . . . ."[123] In an odd twist, the statute allows for the data-collecting business, not the consumer, to recover damages from the party who unlawfully obtained the information and does not provide consumers with a cause of action against the business responsible for the leak.[124] The Nevada statute does not explain what reasonable procedures are, is unclear on the consumer notice requirement, and leaves consumers without an express cause of action.[125]

3. Hustle and Bustle: The New York Approach

New York's data-breach statute is listed in the general business law section of the state's code.[126] The statute is broad in its scope and covers "[a]ny person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information . . . ."[127] The statute does not require businesses that collect information to implement security procedures to protect consumer

117. *See id.* § 17.50(h).
118. *See id.* §§ 521.151(a)–(b), .101.
119. *See id.* § 521.001.
120. NEV. REV. STAT. ANN. § 603A.210 (West 2017).
121. *Id.* § 603A.210(1).
122. *See id.* § 603A.210.
123. *Id.* § 603A.220(1).
124. *See id.* § 603A.900.
125. *See id.* § 603A.210.
126. N.Y. GEN. BUS. LAW § 899-aa (McKinney 2018).
127. *Id.* § 899-aa(2).

information.[128] The statute only addresses notice to consumers after a data breach occurs and mandates that the notice take place "in the most expedient time possible and without unreasonable delay . . . ."[129] Additionally, the statute does not provide consumers with a private cause of action and instead allows the New York Attorney General's office to file suit against businesses that fail to comply with the notice requirement.[130] The state may recover damages on behalf of consumers that result from the failure to provide notice but not for failure to protect the information itself.[131] The New York approach leaves unaddressed the protection of consumer data, focuses primarily on the notice requirement, and, again, leaves consumers with nowhere to turn for recovery of damages.[132] The difficulties faced by consumers and businesses from current data-breach regulations are clear. The following Parts examine an emerging technology that can be used as a preventive measure for data breaches and shows ways that the technology is currently being utilized.

IV. PREVENTING THE SPREAD: THE UNTAPPED POTENTIAL OF BLOCKCHAIN TECHNOLOGY

"We may be at the dawn of a new revolution."[133] Blockchain technology is a new and exciting technological advancement that could fundamentally change the way society functions.[134] Corporations have taken notice of the technology with names like Google, Goldman Sachs, Samsung, and Visa investing significantly into exploring the technology and how it can be applied to their business models.[135] The specific coding and infrastructure of how the technology operates are extensive.[136] For that reason, this

128. *See id.* § 899-aa.

129. *Id.* § 899-aa(2).

130. *See id.* § 899-aa(6)(a).

131. *See id.*

132. *See id.* § 899-aa.

133. MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY, vii (Tim McGovern et al. ed., 2015) (suggesting that blockchain technology has the potential to change modern society similar to when the Internet was first introduced).

134. *See generally id.* (exhibiting excitement about the possible ways that blockchain technology can be used). The original idea for blockchain technology and Bitcoin was published in an anonymously written paper in 2008 under the name Satoshi Nakamoto. *See* Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, BITCOIN.ORG (2008), https://Ibitcoin.org/bitcoin.pdf. The mystery still exists surrounding the identity of the individual who conceptualized the technology. *See* Sophie Bearman, *Bitcoin's Creator May Be Worth $6 Billion — But People Still Don't Know Who It Is*, CNBC (Oct. 27, 2017, 10:43 AM), https://www.cnbc.com/2017/10/27/bitcoins-origin-story-remains-shrouded-in-mystery-heres-why-it-matters.html.

135. *See More Mainstream Companies Invest In Blockchain*, NASDAQ (Mar. 17, 2017, 9:51 AM), http://www.nasdaq.com/article/more-mainstream-companies-invest-in-blockchain-cm762121; Arjun Kharpal, *Google and Goldman Sachs Are Two of the Most Active Investors in Blockchain Firms: Report*, CNBC (Oct. 18, 2017, 6:45 AM), https://www.cnbc.com/2017/10/18/google-goldman-sachs-investors-blockchain.html.

136. Chris Skinner, *Blockchain? It's Complicated*, BANK NXT (Mar. 3, 2016), https://banknxt.com/

Comment only provides a surface-level overview, which discusses what the technology is and how it can be applied.[137]

At its core, a blockchain is essentially a ledger.[138] The ledger records various transactions, time stamps them, and then lumps them into what are known as blocks.[139] Transactions can only be added to the ledger and are highly difficult, if not impossible, to remove.[140] The ledgers are stored throughout a network of computers that work together to verify transactions.[141] The decentralized storage of the ledgers and cooperative nature of the system make it difficult for hackers to attack one computer and successfully alter previous ledgers—if one ledger is altered, the network will see the alteration when referencing previous ledgers and invalidate the fraudulent change.[142] Blocks of transactions are linked to the previous ledgers, which forms a chain.[143] The blocks serve as references to the previous ledgers so that when someone attempts to make a transaction, the transaction is verified by referencing previous ledgers.[144] Once a transaction is validated, the transaction is permanently added to the ledger, and a new ledger is distributed throughout the network as the point-of-reference for future transactions.[145] Because of the decentralized storage of data and collaborative nature of the system, blockchains are highly resilient to data breaches and present a solution to data-protection concerns.[146]

A. Digital Dinero: The Rise of Bitcoin

The largest and most well-known application of blockchain technology is Bitcoin.[147] Many people are familiar with Bitcoin due to its association with "The Silk Road" and the facilitation of online narcotic sales.[148] Others

---

55981/blockchain-its-complicated/ (showing "how complicated, but also exciting, [blockchain] developments are, and the fact that there are so many firms building on this technology demonstrates there's something serious happening here").

137. To reiterate, this Comment does not seek to provide an exhaustive analysis of the technology itself, but only how it can be applied to address and prevent future data-breach incidents.

138. SHAWN S. AMURIAL ET AL., THE BLOCKCHAIN: A GUIDE FOR LEGAL AND BUSINESS PROFESSIONALS § 1:1 at 1 (2016).

139. *Id.* The word "transactions" is very broad in scope and encompasses any type of stored data. *See generally id.* Transactions can include personal records, marriage certificates, wills, contracts, land deeds, car titles, gun ownership, or any other recorded document. *See generally id.*

140. Nakamoto, *supra* note 134, at 1.

141. *See generally* AMURIAL, *supra* note 138.

142. *See generally id.*

143. *See generally id.*

144. *See generally id.*

145. *See generally id.*

146. *See generally id.*

147. *See* SWAN, *supra* note 133, at 1.

148. *See* Nicky Woolf, *Silk Road Sentencing: Why Governments Can't Win the War on Darknet Drugs*, GUARDIAN (May, 31 2015, 7:00 AM), https://www.theguardian.com/technology/2015/may/31/silk-road-sentencing-darknet-drugs (demonstrating the emergence of online drug sales using Bitcoin as a form of anonymous payment).

may know it because of its volatility and increased prevalence in the world of investments and day trading.[149] Regardless of how it is perceived, Bitcoin has by far been the most successful and groundbreaking form of "cryptocurrency," or digital cash, and has the capability to change the way commerce is facilitated.[150] Previous forms of digital currency have been susceptible to "double spending."[151] Typically, a third party, such as a bank, would have been needed to host a ledger and ensure that digital cash was only spent once.[152] The double spending issue has come to be known as the "Byzantine Generals' Problem."[153] Blockchain technology has made the problem nonexistent by ensuring digital cash is only spent once by validating and recording transactions using the decentralized ledger system.[154]

The way a Bitcoin is identified and transferred is one of the most important security aspects of the system.[155] Bitcoin themselves are associated with a public address, which is very similar to a URL address for a website.[156] The public address is generated when the Bitcoin comes into existence, although the possessor of the Bitcoin can change it.[157] Bitcoin are also linked to a "private key."[158] The private key is what a person uses to spend his or her Bitcoin by "signing off" on a transaction.[159] Put simply, a public key can be shared freely with no security risk—the public key only allows a person to view the ledger and verify that the Bitcoin exists.[160] The private key is the tool that authorizes the transaction to take place and must be well protected to ensure that the Bitcoin is secure.[161] In other words, "the Bitcoin at [a] public address can only be spent by having the corresponding private key."[162]

To bring all of this information full circle and illustrate how ingenious the system is, an illustration is instructive. Assume that Alfred wants to pay Bruce in Bitcoin for services rendered. The transaction would start by Alfred

---

149. *See* Jeff John Roberts, *$5,000 Bitcoin? 3 Reasons to Buy—and to Stay Away*, FORTUNE (Aug. 10, 2017), http://fortune.com/2017/08/10/should-i-buy-bitcoin/ (reporting that "a growing number of mainstream investors and entrepreneurs [] see [B]itcoin—and other digital currencies—as a legitimate asset class such as stocks, bonds, or commodities").

150. *See* SWAN, *supra* note 133, at 2–3 (explaining that cryptocurrency is essentially digital cash and "a way of buying and selling things over the Internet").

151. *See id.* at 2.

152. *See id.*

153. *See id.* (noting that the Byzantine Generals' Problem is "the difficulty of multiple parties (generals) on the battlefield not trusting each other but needing to have some sort of coordinated communication mechanism").

154. *See id.*

155. *See* AMURIAL, *supra* note 138, § 1:3 at 1.

156. *See id.*

157. *See id.*

158. *See id.*

159. *See id.*

160. *See id.*

161. *See id.*

162. *Id.* § 1:3 at 2.

giving Bruce the public key to the Bitcoin he possesses.[163] Bruce could then use the public key provided by Alfred to look at the blockchain ledger and verify that Alfred has the Bitcoin he claims.[164] Alfred would then need to initiate the transaction by sending the Bitcoin to Bruce's Bitcoin wallet and then sign off on the transaction using his private key to authorize the transfer.[165] The final step is to "broadcast" the transaction into the Bitcoin network for validation.[166] Once the network reaches consensus that the transaction is valid and properly signed, the transaction is recorded onto the blockchain, and the new ledger is distributed throughout the network reflecting the change in ownership.[167]

B. Endless Possibilities: Alternative Applications of Blockchain Technology

An important distinction exists between Bitcoin and Blockchain technology.[168] The simplest way to make this distinction is to consider the Internet.[169] Much like email and websites utilize the Internet as the vehicle to carry out their services, Bitcoin uses blockchain as the vehicle to carry out its service.[170] The distinction is important because it illustrates that there are numerous other ways blockchain technology can be used.[171]

1. Meeting of the Minds: Blockchain Contracts

In the legal world, blockchain technology is currently being tested for application in "smart contracts."[172] To illustrate, Party A first uploads a contract to the blockchain as a document that requires review, edit, and signature by Party B.[173] The document is then sent to Party B.[174] After Party B makes his adjustments and signs the document, it is then time-stamped, saved to the blockchain, and sent back to Party A for further review, editing, and signature.[175] The process can continue as long as needed, but once the contract terms are finalized, and both parties authenticate the document, the

163. *See id.* § 1:3 at 3.
164. *See id.*
165. *See id.* E-wallets have become a commonly-used means for storing digital currency and are available in software or hardware forms. *Id.*
166. *See id.* A "node" is the term used to describe one of the many computers in the network that validate and monitor transactions. *Id.*
167. *See id.*
168. *See* SWAN, *supra* note 133, at 9.
169. *See id.*
170. *See id.*
171. *See id.*
172. *See id.*
173. *See id.* at 10.
174. *See id.*
175. *See id.*

contract is recorded on the blockchain once more and forever memorialized.[176] Another possibility is to have a conditional contract "where a transaction occurs when some conditions are fulfilled."[177] The conditional contract would serve a similar role to an escrow agent in which the contract would not be recorded until a certain amount of time passes, money is paid, or some other condition is met.[178] Because blockchains are time-stamped, recorded, and validated throughout a network, commonly disputed contract issues can be avoided.[179]

2. Seamless Transfer: Blockchain Property Transactions

Technology analysts around the globe are also exploring the concept of applying blockchain technology to "smart property."[180] Smart property is very similar in application to a Bitcoin transaction and can be applied to any property, whether personal or real.[181] For example, "[a]ny asset can be registered in the blockchain, and thus its ownership can be controlled by whoever has the private key [to the asset]."[182] The process for the transaction would be virtually identical to a Bitcoin transaction in which parties must use their private key to sign off on an asset transfer.[183] The added security of a private key that requires the granting party to sign off on a transaction would provide a level of trust and security between the parties that often lacks in property transfers.[184] Blockchain technology can exponentially facilitate the process of determining ownership and transferring rights while combatting fraud, crime, and other ownership disputes.[185]

---

176. *See id.*

177. Garry Gabison, *Policy Considerations for the Blockchain Technology Public and Private Applications*, 19 SMU SCI. & TECH. L. REV. 327, 345 (2016).

178. *See id.*

179. *See* SWAN, *supra* note 133, at 10 (referring to contract claims such as incomplete terms, fraud, lack of consideration, etc.).

180. *See id.* at 14; *see also The Trust Machine*, THE ECONOMIST (Oct. 31, 2015), https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine (noting that Honduras and Greece have begun to investigate how to apply blockchain technology to property ownership registries).

181. *See* SWAN, *supra* note 133, at 14. Blockchain technology can be applied to ownership in land and property titles, vehicle registrations, business licenses, stock, private equity, patents, trademarks, etc. *Id.* at 10.

182. *Id.* at 14; *The Trust Machine*, *supra* note 180 (explaining that "[d]ocuments can be notarised by embedding information about them into a public blockchain—and you will no longer need a notary to vouch for them").

183. *See supra* text accompanying notes 163–67 (providing an example Bitcoin transaction).

184. *See* SWAN, *supra* note 133, at 14–15.

185. *See id.* Using blockchain technology, familiar issues in property transactions such as uncertainty of title, determination of ownership, fragmentation of interests, searches of deed records, and extensive title searches can all be avoided. *See generally id.*

C. Productivity Unleashed: Blockchain Government

Blockchain technology can create a more efficient and effective administration of governmental services.[186] For example, citizen identification cards, land deeds, marriages, wills, tax records, and business incorporations can all be logged and submitted to a private blockchain network ensuring safe and secure storage.[187] Technology experts suggest that using the blockchain in this way will save governments both time and resources, which can instead be applied to situations that require human interaction.[188] However, while the upside is significant in adopting a record-keeping system based on blockchain technology, some argue that the cost-benefit analysis weighs in favor of maintaining the current system.[189] The following Section highlights the success that a small European country, Estonia, has had in using blockchain technology to facilitate many of its governmental services and shows how the blockchain system has allowed the country to operate free from data-protection issues.

D. The Blockchain Nation: Estonia

Estonia is a small European country with an estimated population of 1.3 million.[190] After regaining its independence in 1991, Estonia had a unique vision for its new society—infrastructure and government centered on technology.[191] It has done just that.[192] Essentially all of Estonia's governmental services are available online.[193] The services are maintained on a blockchain technology-based information-sharing system, known as the X-Road, which allows governmental agencies and businesses to seamlessly and securely share records.[194] The success of putting the Estonian system in

186. *See id.* at 48.

187. *See id.* at 48–49.

188. *See id.* at 46–47.

189. *See* Gabison, *supra* note 177, at 328 (explaining the advantages and disadvantages of using blockchain technology in governmental roles).

190. *Facts about e-Estonia*, REPUBLIC OF EST. INFO. SYS. AUTHORITY, https://www.ria.ee/en/facts-about-e-estonia.html (last visited Mar. 4, 2018).

191. *See id.* ("Therefore the keywords behind the development of e-State in Estonia are sustainable development and high-quality environment."); Patrick Kingsley, *How Tiny Estonia Stepped Out of USSR's Shadow to Become an Internet Titan*, GUARDIAN (Apr. 15, 2012, 1:51 PM), https://www.theguardian.com/technology/2012/apr/15/estonia-ussr-shadow-internet-titan.

192. Walt, *supra* note 15.

193. *E-Identity*, E-ESTONIA, https://e-estonia.com/solutions/e-identity/id-card/ (last visited Mar. 4, 2018) [hereinafter *E-identity*] (listing available uses including: "legal travel ID for Estonian citizens traveling within the EU[;] national health insurance card[;] proof of identification when logging into bank accounts[;] for digital signatures[;] for i-Voting; to check medical records, submit tax claims, etc.[;] to use e-Prescriptions").

194. *Success Stories: X-Road*, E-ESTONIA, https://e-estonia.com (last visited Mar. 5, 2018) [hereinafter *Success Stories: X-Road*] ("This is the invisible yet crucial environment that allows the nation's various e-service databases, both in the public and private sector, to link up and operate in harmony, and saves more than 800 years of working time for the state and citizens annually.").

place depended largely on two things: the country had to (1) develop a state-sponsored digital identification card for use by its citizens, and (2) develop a system that allowed governmental agencies to securely share information.[195] This Section will focus on the digital identification cards, the data-security advantages of the X-Road, and the quality of life that Estonians enjoy as a result of their comprehensive data system.

1. Identity Protected: Digital Identification Cards

In 2001, Estonia launched its first nationwide digital identification card (ID card).[196] The ID cards allow citizens to prove identity, digitally sign documents, and access the country's numerous government services available online.[197] Each card is fitted with a micro-chip that is compatible with a standard smart-card reader and allows the use of "two core functionalities provided by the ID-card, both of which are essential to the development of e-government—personal authentication [] and digital signature []."[198] The card user assigns the two functions with a separate PIN number, which allows for secure individual use.[199] The authentication component of the card simply allows for proof of identity.[200] The signature component allows citizens to effectuate a legally binding signature.[201] Card use has been widely adopted in everyday Estonian life, and even the Estonian Prime Minister utilizes the card's electronic signature function to enact legislation.[202]

2. Safe and Secure: The X-Road

The X-Road is Estonia's solution to allowing governmental agencies and private businesses to share records and information safely, securely, and efficiently.[203] To make the system work, people, land properties, addresses, and businesses are assigned a numerical identifying number and recorded in

---

195. KRISTJAN VASSIL, WORLD DEV. REP., ESTONIAN E-GOVERNMENT ECOSYSTEM: FOUNDATION, APPLICATIONS, OUTCOMES, 2016, at 2, 11 (June 2015), http://pubdocs.worldbank.org/en/16571145683 8073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf.

196. *Facts about e-Estonia*, *supra* note 190; *Estonia Takes the Plunge*, ECONOMIST (June 28, 2014), https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge. Now, the system has become such a staple of Estonian society that "before a newborn even arrives home, the hospital will have issued a digital birth certificate and his health insurance will have been started automatically." *Estonia Takes the Plunge*, *supra* note 196.

197. *See E-Identity*, *supra* note 193.

198. VASSIL, *supra* note 195, at 4.

199. *See id.*

200. *See id.*

201. *See id.*

202. *See* Walt, *supra* note 15.

203. *See Interoperability Services*, E-ESTONIA, https://e-estonia.com/solutions/interoperability-services/x-road/ (last visited Mar. 5, 2018) [hereinafter *Interoperability Services*].

the government system.[204] When one set of data changes, such as a person's address or the birth of a child, the system interconnects and communicates the change to update other affected records.[205] The X-Road facilitates the efficient communication of data between government agencies so that up-to-date records are maintained.[206]

Utilizing key features of blockchain technology, "all outgoing data from [the] X-Road is digitally signed and encrypted, and all incoming data is authenticated and logged."[207] The X-Road incorporates the use of Estonia's government-issued digital IDs, and all inquiries through the ID are time-stamped and recorded so that Estonian citizens can see who accessed their records, when they did, and for what purpose.[208] One of the core reasons that Estonia elected to adopt the X-Road system lies in the fundamental idea of decentralizing data storage.[209] The dangers in a centralized data system stem from the problem of having "all your eggs in one basket."[210] The X-Road alleviates this problem by dispersing collected data to separate government agencies and prohibiting the collection of duplicate data.[211] Because of the X-Road system, Estonians can have peace of mind that their society is operating efficiently and securely and avoid issues, like data breaches, which come from poor data-sharing and data-protection practices.

3. Freedom from Data Worries: Life in the Blockchain Nation

Estonia has enjoyed unprecedented success in its vision for a digital society.[212] To carry its goals further, the Estonian government has now deemed Internet access to be a basic human right allowing for ease of citizen access to online services.[213] Voting in elections, receiving medication prescriptions, filing tax returns, and paying for goods, are all regularly carried out via a computer.[214] Thanks to their digital system based on blockchain technology, citizens claim that they feel more secure than if things were done

---

204. *See* Anto Veldre, *Introduction to X-Road (Part 1)*, REPUBLIC OF EST. INFO. SYS. AUTHORITY (Sept. 2, 2016), https://www.ria.ee/en/introduction-to-xroad-part1.html.

205. *See id.*

206. *See id.*

207. *See Interoperability Services*, *supra* note 203. A record always exists of when a request for data is made and when it is granted. *See id.*

208. *See id.* This feature helps alleviate the fear of identity fraud and the unauthorized access of private records. *See id.*

209. Veldre, *supra* note 204.

210. *Id.* (citing the dangers of centralizing data storage such as the destruction of records, security issues from cyber-attacks and data breaches, and government monopoly of citizen records).

211. *See id.* Barring the collection of duplicate data, such as a person's date of birth, helps alleviate security concerns because citizens do not have to worry that multiple agencies have access to their information. *See id.*

212. *See* Kingsley, *supra* note 191.

213. *See id.*

214. *See id.*

in an offline manner.[215] One Estonian commented, "If anyone goes into my files, they're flagged. Whereas if my files—which would exist anyway—were made of paper, no one would know who was looking at them."[216] Government officials estimate that the blockchain-based X-Road has saved "800 years of working time for the state and citizens annually."[217] Setbacks have occurred since the system began operation, but for the most part, the country has enjoyed the benefits of a digital society without issue.[218] This year, the country "will open the world's first 'data embassy' in Luxembourg—a storage building to house an entire backup of Estonia's data that will enjoy the same sovereign rights as a regular embassy but be able to reboot the country remotely . . . ."[219] Though some argue that Estonia's model is not scalable to accommodate large populations, Estonia presents an interesting example of what life can look like when technology-based policies are placed at the forefront of government priority.[220]

V. THE PRACTICAL SOLUTION: UNIFORMITY, RELIEF, AND PREVENTION

The United States data-breach epidemic imposes significant financial costs on all parties involved and places consumers in a constant state of fear of possible identity fraud.[221] The United States must take a proactive, rather than reactive, approach to data-security issues.[222] The proactive approach must be comprehensive and must start by addressing the shortcomings of current data-breach regulations.[223] Current regulations do not cover all entities that collect consumer information; they provide vague data protection standards and little guidance to businesses that collect consumer data; they suggest inconsistent consumer notification requirements after a data-breach occurs; and they often leave consumers without an express cause of action.[224] The first step to addressing the data-breach epidemic is for federal legislators to enact an all-encompassing data-protection and data-breach notification statute.[225] Next, policymakers at all levels of government must consider utilizing new solutions, such as blockchain technology, in governmental roles

---

215. *See id.*

216. *Id.* A level of record security is achievable due to the time-stamping and recording of blockchain technology. *See* Nakamoto, *supra* note 134, at 1.

217. *Success Stories: X-Road*, *supra* note 194.

218. *See* Walt, *supra* note 15.

219. *Id.*

220. *See id.*

221. *See supra* text accompanying notes 40–48 (showing costs incurred by consumers and businesses following a data breach).

222. *See generally supra* Part III (analyzing the problems with current data-breach regulations).

223. *See supra* text accompanying notes 61–65 (recognizing the complications and inconsistencies in current data-breach law).

224. *See generally* Mank, *supra* note 65; Peters, *supra* note 61.

225. *See supra* text accompanying notes 75–85 (comparing proposed federal legislation on data-protection and data-breach concerns).

to mitigate and prevent future data breaches.[226] This Part outlines the fundamental attributes that must be included in a federal data-breach and data-protection statute and suggests two ways blockchain technology could be used at federal and state levels.

A. Strict and Uniform: Federal Data-Breach and Data-Protection Regulations

Federal legislators can begin to address the data-breach epidemic by enacting a uniform data-breach notification and data protection statute that preempts all state data-breach law. The statute should designate the FTC as the promulgator of regulation concerning consumer data collection and should create a specific department for cybersecurity.[227] The FTC is the appropriate agency for consumer data regulations because of its direct involvement in interstate commerce and business regulation.[228] By creating a specialized department for cybersecurity, regulations would be enacted and enforced by a governing body that specializes in data-breach and data-protection matters, and the department could also serve as a resource that businesses can turn to for guidance on data-breach related issues.

1. Expansive Scope: Applicable Entities and Personal Information Defined

The statute should be broad in coverage and include all persons and businesses in the United States that collect personal and sensitive consumer information. Personal information should be defined broadly in the statute and include names, birthdates, Social Security numbers, addresses, and any other personal information relating to the identity of consumers.[229] The covered entities language of the statute should be similar to the New York data-breach notification statute and mirror its sweeping language.[230] The language of the statute could read: "*Any person or business* which conducts business in the United States, and *collects private consumer information*, is subject to the regulations of this statute." By covering all businesses that collect private information, the statute would close the gap of covered

226. *See supra* Section IV.D (examining how Estonia has used a blockchain-based information sharing system to fulfill governmental functions).

227. *See supra* text accompanying note 78–80 (discussing legislation that would require businesses to implement data-breach measures and provide timely disclosure upon the occurrence of a data breach).

228. *See About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc (last visited Mar. 19, 2018) (outlining the FTC's mission to "protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity").

229. *See generally* Peters, *supra* note 61 (discussing the similarities in how states define personal information in data-breach notification statutes).

230. *See supra* text accompanying note 127 (explaining how the New York statute covers virtually all entities conducting business in the state).

industries that is left open by current state and federal regulations.[231] The broad definition and sweeping coverage will allow consumers to feel secure that any person or business collecting their personal information will be subject to federal oversight.[232] Additionally, businesses will have clear regulations and know who is enforcing them.[233]

2. Guidance and Clarity: Data-Protection Standards

The commonly used "reasonable procedures" language applying to consumer dataprotection must no longer be the standard.[234] Instead, the statute should vest authority to the cybersecurity department of the FTC and allow the department to specify minimum-security measures that must be implemented by entities subject to the statute.[235] The cybersecurity department must address the lack of guidance businesses currently face and should be responsible for outlining ways that businesses can assess their current data-protection procedures and combat their vulnerability for future data breaches.[236] Additionally, the department should provide best practice measures on how businesses can adjust their current data-protection procedures to comply with the minimum-security requirements. These provisions will alleviate the confusion and lack of clarity that businesses face because of the inconsistencies in current data-breach and data-protection laws.[237]

3. Timely Disclosure: Data-Breach Notification Requirement

The statute must address the consumer data-breach notification issue by requiring covered entities to follow a uniform notification requirement and a specified time of disclosure.[238] The statute should not allow businesses to defer to their own disclosure requirements.[239] Businesses must be required to notify all affected consumers of a data-breach occurrence that results in personal information disclosure.[240] The required time of notification should

---

231. *See* discussion *supra* Section III.A (discussing the lack of uniformity in data-breach law in the United States).

232. *See* discussion *supra* Section II (highlighting the vulnerability of consumers' personal information after credit-reporting agencies collect and compile credit reports).

233. *See* N.Y. GEN. BUS. LAW § 899-aa(2) (McKinney 2018).

234. *See* TEX. BUS. & COM. CODE ANN. § 521.052(a) (West 2017).

235. *See* Data Breach Prevention and Compensation Act of 2018, S. 2289, 115th Cong. (2018).

236. *See* discussion *supra* Sections III.A, III.C (pointing out the lack of guidelines in current federal and state data-breach laws).

237. *See* discussion *supra* Sections III.A, III.C (explaining the varied approaches of current statutes).

238. *See* discussion *supra* Sections III.A, III.C (showing the inconsistent time of disclosure required by current federal and state data-breach laws).

239. *See* discussion *supra* Sections III.A, III.C (describing how current data-breach regulations sometimes allow businesses to defer to their own data-breach notification procedures).

240. *See* discussion *supra* Sections III.A, III.C (providing the varied requirements of who businesses

be no longer than thirty days after a data breach occurs. The thirty-day period will provide businesses with ample time to assess a possible breach, determine the scope of information compromised, and compile lists of consumers that must be notified. By providing a specific time for disclosure, the statute will address the vague language of current laws, which often allow businesses to notify consumers at their own discretion.[241] The statute will allow consumers to be equipped with an understanding that their information has been exposed so they can take appropriate measures to protect their identities.

4. Remedies Amended: A Private Cause of Action and Disclosure Penalties

Consumers must be provided with a private cause of action against companies who fail to protect their private information.[242] Under the current scheme of data-breach regulations, state and federal law often leave consumers without a remedy and courts are split as to whether the mere disclosure of information is enough to satisfy standing to bring suit.[243] The statute should be clear that any personal consumer information disclosed in a data breach satisfies standing, and the information does not need to be used fraudulently for a consumer to seek damages.[244] The express cause of action will provide certainty that companies can be held accountable for their failure to protect personal information and will alleviate the issue of proving standing.[245] Additionally, the statute should impose significant civil penalties against companies who do not comply with federal data-breach regulations.[246] The statute should also make companies criminally liable for willfully or knowingly violating the statute.[247] The remedies and penalties included in the statute will ensure that businesses make data-breach prevention and regulation compliance a top priority and that if they do not, significant consequences will follow.[248]

---

must notify after a data breach occurs).

241. *See* discussion *supra* Sections III.A, III.C (showing how current laws fail to require businesses to disclose a data breach within a specific time period).

242. *See* discussion *supra* Sections III.A, III.C (describing the lack of remedies for consumers in current federal and state data-breach laws).

243. *See* discussion *supra* Section III.B (analyzing the differing ways that courts interpret the standing requirement in data-breach litigation).

244. *See* discussion *supra* Section III.B (discussing the difficult standing requirements of current law).

245. *See* discussion *supra* Sections III.A, III.C (outlining the lack of consumer remedies in current data-breach regulations).

246. *See supra* notes 78–80 and accompanying text (considering proposed federal legislation that would impose civil and criminal liabilities on companies that violate federal data-security regulations).

247. *See* Consumer Privacy Protection Act of 2017, S. 2124, 115th Cong. (2017) (proposing criminal charges for companies who willfully violate data-breach disclosure requirements).

248. *See* discussion *supra* Part III (exposing the inadequacies of current data-breach regulations).

B. Charging Forward: Blockchain Technology in Governmental Roles

Federal and state legislators should also consider the adoption of blockchain technology to safely store and secure government records. Blockchain technology provides a high level of data security by decentralizing storage of sensitive information.[249] Additionally, blockchain ledgers are time-stamped and recorded, which allows users to see information that has been accessed or changed.[250] The United States should consider implementing a system similar to Estonia's to ensure that government data is safeguarded, verified, and recorded, which would allow the government to operate more efficiently and allow citizens to verify that their information is accessed only for proper purposes by proper individuals.[251]

1. Digital Identity: Blockchain Technology at the Federal Level

At the federal level, an ideal area for blockchain technology to be utilized is in digital ID cards.[252] The use of Social Security cards as a means of proving identity should be phased out due to its rampant risk for identity fraud.[253] The federal government could initiate the process by outfitting all newly issued passport cards with a microchip that allows citizens to prove identity.[254] Citizen information could be collected and stored at various federal offices throughout the country with each office storing citizen information only on individuals who live in the state where the office is located.[255] The offices could act in a collaborative blockchain manner, similar to the Estonian X-Road, where information is exchanged, verified, and recorded.[256] The system should also allow for citizens to access a personal account associated with their card detailing when requests are made, who makes them, and when they are granted.[257] The personal account feature will ensure that authorized individuals only access citizen information for

---

249. *See* discussion *supra* Sections IV.C, IV.D (establishing the benefits of using blockchain technology in governmental roles).

250. *See supra* text accompanying notes 138–146 (discussing how blockchain technology works and the security features that the system utilizes).

251. *See* discussion *supra* Section IV.D.2 (complimenting the Estonia X-Road system that allows for government records to be shared without data-security issues).

252. *See* discussion *supra* Section IV.D.1 (examining Estonian digital identification cards).

253. *See supra* text accompanying notes 51–54 (criticizing the use of Social Security cards as identification).

254. *See Passport Card*, U.S. DEP'T OF ST.—BUREAU OF CONSULAR AFF., https://travel.state.gov/content/travel/en/passports/apply-renew-passport.html (last visited Mar. 6, 2018).

255. *See Passport Agencies*, U.S. DEP'T OF ST.—BUREAU OF CONSULAR AFFS., https://travel.state.gov/content/travel/en/passports/requirements/where-to-apply/passport-agencies.html (last visited Mar. 6, 2018) (identifying U.S. passport offices); *see also supra* text accompanying note 211 (giving an example of how Estonia's X-Road system implements this strategy to meet this challenge).

256. *See supra* text accompanying note 208 (detailing how the X-Road system operates).

257. *See supra* text accompanying note 208 (examining this exact operating system).

proper purposes.[258] By starting with an ID card, government officials can experiment with the technology and address any issues with the system. Passports are ideal for experimentation because they would not interfere with any of the traditional ways that Americans currently prove identity.[259] If the system proves effective and efficient, officials can then move towards adding additional user features to the ID cards.[260]

2. Superior Democracy: Voting in the States with Blockchain Ballots

At the state level, legislators should consider using blockchain technology for voting in elections.[261] Newly issued state voter cards could come with the option to create an online profile and private key, which then could be used to vote on a blockchain ledger.[262] The private key could be utilized via a smartphone, computer, or at a traditional voting booth.[263] Allowing citizens to vote digitally could increase voter turnout, combat voter fraud, and ensure that votes are counted accurately.[264] Various databases could be set up in states that verify, compare, and record, using the blockchain system to ensure the integrity of the voting system is upheld.[265] Voters should not be required to vote digitally, but should be able to participate if they choose. If the system proves to be successful, state officials could then move toward exploring additional applications of blockchain technology in government roles such as recording property ownership, marriage certificates, and state-issued driver's licenses.[266]

3. Committing to the Cause: Complexities of the Blockchain System

While the upside to blockchain technology is significant, officials will also need to address some of the hurdles in using a blockchain system.[267] One issue that would need to be addressed is the computing power required to run

---

258. *See supra* text accompanying note 208 (discussing this purpose as one of the benefits of a system such as the X-Road system).

259. *See* discussion *supra* Section II.C (discussing the variety of ways United States citizens prove identity).

260. *See supra* text accompanying note 195 (giving examples of such additional features added by Estonia); *supra* text accompanying note 201 (discussing how Estonia allows the signature component of its ID cards to execute a legally binding signature).

261. *See supra* note 193 and accompanying text (discussing how Estonia conducts multiple governmental functions online).

262. *See* Gabison, *supra* note 177, at 347.

263. *See id.* at 348.

264. *See id.* at 347–48.

265. *See id.*

266. *See supra* text accompanying note 220 (discussing how Estonia could be a model for establishing a blockchain system in the United States).

267. *See generally* Gabison, *supra* note 177 (weighing the policy considerations of using blockchain technology in governmental roles).

the system.[268] Blockchain systems operate in a collaborative nature and continually reference previous ledgers to ensure that additions to the chain are authorized.[269] The process of verifying, recording, and exchanging information requires a significant number of computers.[270] Additionally, powering the required computers consumes a significant amount of energy.[271] Officials would need to determine ways to acquire the computing power and energy to make the system operate.[272] The continued emergence of new and efficient computing technology and the growth of eco-friendly energy options should provide adequate solutions to these issues, if officials will commit to the system overhaul.[273]

VI. OVERCOMING THE CRISIS: THE DAWN OF A NEW AGE

Data breaches have proven to be a consistent problem in the United States.[274] State and federal regulations do not address the problem in a way that grants consumers and businesses clarity on their respective rights and duties after a breach occurs.[275] Consumers face uncertainty in seeking relief after their information is exposed, and conflicting laws relating to compliance burden businesses.[276] Blockchain technology presents an opportunity to prevent and mitigate future data-breaches by decentralizing data storage and utilizing a ledger-based system to ensure information is recorded, time-stamped, and verified.[277] The blockchain system could fundamentally change the way society functions and could be adopted into United States culture to make everyday life more safe and efficient.[278]

Enacting a federal data-breach notification and data-protection statute would alleviate the deficiencies of the current regulatory scheme.[279] The legislation would provide clarity to businesses on compliance, risk assessment, and data-protection issues.[280] Additionally, consumers would be able to receive notification of data-breaches and seek damages from

---

268. *See id.* at 341.
269. *See id.*
270. *See id.*
271. *See id.* at 342.
272. *See id.*
273. Skye Hudson, *Top 10 Emerging Technologies That Are Changing the World*, MAKEUSEOF (Sept. 15, 2014), https://www.makeuseof.com/tag/top-10-emerging-technologies-changing-world/ (identifying new and emerging technologies to tackle energy, health, and other societal issues).
274. *See supra* Part II (discussing the existence of such breaches throughout the United States).
275. *See supra* Sections III.A, III.C (discussing the lack of consistency or regularity regarding such state and federal regulations).
276. *See supra* Part III (detailing the uncertainty after a breach).
277. *See supra* Part IV (explaining the ledger-based system and its advantages).
278. *See supra* Part IV (explaining the advantages of the blockchain system).
279. *See supra* Section V.A (discussing how this type of legislation would meet the current gaps in the law).
280. *See supra* Section V.A.2 (explaining options to give businesses more guidance).

businesses that leak their personal information.[281] The legislation would also allow for sanctions to be levied against businesses that fail to comply with federal regulations.[282] In the future, state and federal governments should also consider using blockchain technology to facilitate government services.[283] Federal ID cards and state elections are prime areas in which blockchain technology could be utilized.[284] The data-breach epidemic is a problem that will not go away overnight, but by codifying well-informed policies, implementing proactive measures, and adopting the use of new technology, the United States can overcome the epidemic and emerge, once again, as the most technologically advanced country in the world.

281. *See supra* Section V.A (examining possible solutions to current gaps in the law).

282. *See supra* Section V.A.4 (detailing specific examples of the possible solutions by identifying possible remedies for victims of data breaches).

283. *See supra* Section V.B (discussing the advantages of the blockchain system).

284. *See supra* Section V.B (examining these areas in closer detail).