July 2019

It's Time for an American (Data Protection) Revolution

Mark Peasley

IT'S TIME FOR AN AMERICAN (DATA PROTECTION) REVOLUTION

*Mark Peasley**

ABSTRACT

The European Union's General Data Protection Regulation is the most comprehensive, far-reaching, and forward-thinking piece of

legislation to be passed in recent history. The GDPR will set the European Union far ahead of the United States when it comes to protecting personal information, but fear not; many of the GDPR's requirements reach across the Atlantic and will offer a trickle-down benefit to United States citizens as entities move towards compliance. However, this is only an unintended benefit of the GDPR. Currently, the United States takes a piecemeal approach to data protection that focuses on the type of information stored, which overlooks the risks that arise when personal information can be collated from multiple, less protected sources.

More is needed from Congress to drive the United States to protect personal information on an overarching level. Some Congressional action has attempted to further the United States' laws regarding data protection, but each attempt in recent history has failed. The United States has two options: stumble forward with its current piecemeal method of data protection or follow its European counterparts with modern, ambitious, and aggressive protection for all of its citizens.

I. INTRODUCTION

From mid-May to July 2017, the credit reporting giant Equifax suffered a data breach in which 143 million consumers' personal information was exposed.[1] To put that number in perspective, there were 127 million working adults in the United States in August 2017.[2] The number of people who had their information exposed is more than the working population of the United States and included most of the United States' adult population.[3] The hack exposed names, social security numbers, birth dates, addresses, and some driver's license numbers.[4]

* Mark Peasley is a graduating 3L at the University of Akron School of Law.

1. Seena Gressin, *The Equifax Data Breach: What to Do, Federal Trade Commission*, FTC CONSUMER INFO. BLOG (Sep. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/9VXB-9M3E].

2. Bureau of Labor Statistics, *Monthly number of full-time employees in the United States from January 2018 to January 2019 (in millions, unadjusted)*, STATISTICA, https://www.statista.com/statistics/192361/unadjusted-monthly-number-of-full-time-employees-in-the-us/ [https://perma.cc/756H-4R5L].

3. Adam Kelsey, *What to know about the Equifax data breach*, ABC NEWS (Sep. 8, 2017, 4:28 PM), https://abcnews.go.com/US/equifax-data-breach/story?id=49701436 [https://perma.cc/8FAQ-NTDS].

4. Gressin, *supra* note 1.

Though Equifax discovered the hack of their database on July 29, 2017, it delayed announcing the breach until September 7, 2017.[5] Following the announcement, Equifax set up a website to allow consumers to check if their data had been stolen.[6] However, the website contained an arbitration clause, which stated that people who logged onto the website waived their right to participate in class-action lawsuits.[7] Equifax later claimed that the arbitration waiver did not apply to those trying to determine if they were a victim of a breach.[8] Sadly, these breaches are not uncommon in today's world where consumers can purchase nearly everything online, including groceries.[9] In 2016, data breaches reached a record high to date, with 1,091 tracked breaches—a 40% increase in breaches from 2015.[10]

Data breaches can be the first step towards identity theft. *Identity theft* is defined as "the unauthorized use of another person's personal information to achieve illicit financial gain."[11] Identity theft victims

5. *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sep. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 [https://perma.cc/57GE-D8NR].

6. Lydia Ramsey, *People are Furious About the Site Equifax Set Up to Let You Know Whether Your Personal Details Were Hacked*, BUS. INSIDER (Sep. 8, 2017, 12:07 PM), http://www.businessinsider.com/equifax-data-breach-site-check-angry-response-2017-9 [https://perma.cc/5TVF-S2YC].

7. *See id.* (stating that if an individual logged in to determine if they were affected by the breach, they waived their right to sue. Individuals were in a catch-22 in that they needed to know if they had been affected to see if they could sue, but by checking to see if they were affected, they would waive their right to sue).

8. *Id.* (stating that Equifax "clarified" the website due to intense backlash from the public).

9. *See, e.g.*, AMAZON PRIME PANTRY, https://www.amazon.com/gp/pantry/info [https://perma.cc/G2HM-RG2L]. Amazon Prime Pantry allows for groceries to be delivered to an address either following an order or on a recurring basis. *Id.*

10. *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RES. CTR, https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/ [https://perma.cc/3W5V-UN79]. The Identity Theft Resource Center is a non-profit entity "established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cyber security, scams/fraud and privacy issues." *About Us*, IDENTITY THEFT RES. CTR, https://www.idtheftcenter.org/about-us/ [https://perma.cc/4FVS-25X2].

11. *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new [https://perma.cc/T3ES-E32B]. Javelin is a research-based advisory firm, offering banking advising for retail companies, small businesses, and digital financing as well as custom research. *See About Javelin*, JAVELIN, https://www.javelinstrategy.com/content/about-javelin [https://perma.cc/VF4W-UBYN] *and* Services offered, JAVELIN, https://www.javelinstrategy.com/ [https://perma.cc/BDN5-K97B] (from the Javelin homepage, place the cursor over the "Services" drop down menu).

suffered 16 billion dollars in losses in 2016.[12] That 16 billion dollars was stolen from 15.4 million United States consumers for an average loss of approximately 1,000 dollars per victim or approximately 6.15% of the total number of United States consumers.[13] The most common type of identity theft is new account fraud, which is when a thief creates a new account (such as a credit card, loan, etc.) using the victim's stolen information.[14] A new, rising area of identity theft is *card-not-present fraud*, where the thief uses the victim's credit card information online.[15]

Up until the Equifax hack, it seemed like the trend had been shifting from personal record exposure toward business record exposure, as the number of personal records exposed had decreased from 169.9 million records in 2015 to 36.6 million records in 2016.[16] Personal identity theft is still common and is usually perpetrated through hacking, skimming, or phishing.[17] While skimming and phishing can result in identity theft, hacking is usually what garners the most attention—like in the Equifax breach.

Additionally, there is no easily discernible trend as to what sort of companies are at the highest risk of data breaches.[18] There have been several high-profile breaches affecting different types of entities in the last five years that have continued to push data breaches into the public attention. The following breaches are examples of high-profile breaches, and the list is by no means exhaustive. In 2013, Yahoo's accounts were breached with over three billion accounts accessed in one of the largest breaches to date.[19] In 2014, Home Depot was breached with 53 million

12. *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST, http://www.iii.org/fact-statistic/identity-theft-and-cybercrime [https://perma.cc/6PB6-ABJQ]. The Insurance Information Institute is a private organization that provides educational information on the insurance industry. *About Us*, INSURANCE INFO. INST., http://www.iii.org/fact-statistic/about-us [https://perma.cc/4973-794Y]. The organization offers membership options for businesses, students, schools, and other groups; membership allows for constant access to the organization's research database, beyond the freely published information. *Membership*, INSURANCE INFO. INST., https://iiimembership.org/ [https://perma.cc/8F7K-QV7Y].

13. JAVELIN, *supra* note 12.

14. INSURANCE INFO. INST., *supra* note 13.

15. JAVELIN, *supra* note 12 (stating that card-not-present fraud has increased 40%).

16. INSURANCE INFO. INST., *supra* note 13.

17. IDENTITY THEFT RES. CTR, *supra* note 10.

18. Elizabeth Weise, *USA Today's list of the biggest data breaches and hacks of all time (Hint: Uber's only #12)*, USA TODAY (October 3, 2017, 5:17 PM), https://www.usatoday.com/story/tech/2017/10/03/biggest-data-breaches-and-hacks-all-time/729294001/ [https://perma.cc/M637-HZK4].

19. Jonathan Stemple & Jim Finkle, *Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft*, REUTERS (October 3, 2017, 4:57 PM), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1 [https://perma.cc/ME3X-B8PF].

accounts accessed[20] and eBay suffered a breach with 145 million victims.[21] In 2015, the U.S. Office of Personnel Management was breached compromising information belonging to almost four million federal employees including names, social security numbers, addresses, and dates of birth.[22] In 2016, breaches included Myspace at 360 million victims[23] and Verizon's data breach contractors, a group created to help other companies with data breaches.[24] Finally, in 2017, FriendFinder Network was breached leading to mass media coverage due to the Network including entities such as AdultFriendFinder, Penthouse, and other adult websites.[25]

The growing threat of database breaches is not just limited to the United States. In response to the breaches, the European Union enacted the General Data Protection Legislation (GDPR) in the summer of 2016 to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[26] The GDPR is an example of comprehensive data security legislation that will be more effective in minimizing data breaches than current U.S. laws, even though certain proposed U.S. laws could rectify some of the U.S.'s shortcomings in the area of data security. The United States should abandon its piecemeal approach toward data security and emulate the GDPR if there

20. *See* Brett Hawkins, *Case Study: The Home Depot Data Breach*, SANS INST. INFOSEC READING ROOM (Jan. 2015), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-home-depot-data-breach-36367 [https://perma.cc/X57M-TV35] .

21. Don Reisinger, *eBay hacked, requests all users change passwords*, CNET (May 21, 2014, 5:30 AM), https://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/ [https://perma.cc/HMC2-AMYB]; *See also* Jim Finkle, *Hackers Raid eBay in Historic Breach, Access 145 Million Records*, REUTERS (May 21, 2014, 11:01 PM), https://uk.reuters.com/article/uk-ebay-password/hackers-raid-ebay-in-historic-breach-access-145-million-records-idUKKBN0E10ZL20140522 [https://perma.cc/D8NT-DZUN].

22. Sam Sanders, *Massive Data Breach Puts 4 Million Federal Employees' Records At Risk*, NPR (June 4, 2015, 7:22 PM), https://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk [https://perma.cc/GJL7-U2M2].

23. Sarah Perez, *Recently Confirmed Myspace Hack Could be the Largest Yet*, TECHCRUNCH (May 31, 2016), https://techcrunch.com/2016/05/31/recently-confirmed-myspace-hack-could-be-the-largest-yet/ [https://perma.cc/QX8M-W69C].

24. Robert Hackett, *Verizon's Data Breach Fighter Gets Hit With, Well, a Data Breach*, FORTUNE (March 24, 2016), http://fortune.com/2016/03/24/verizon-enterprise-data-breach/ [https://perma.cc/DY2W-5JDJ] (stating that Verizon Enterprise, a division of which whose mission is to advise companies on how to respond to a data breach was breached, with 1.5 million customer records accessed).

25. Megan Rose Dickey, *FriendFinder Networks Hack Reportedly Exposed Over 412 Million Accounts*, TECHCRUNCH (November 13, 2016), https://techcrunch.com/2016/11/13/friendfinder-hack-412-million-accounts-breached/ [https://perma.cc/9LCR-K22Z].

26. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter General Data Protection Regulation].

is to be any true progress across the board for U.S. citizens and the security of their personal information. This article will compare the recently passed GDPR with current and proposed United States data protection laws to show where the United States is behind the European Union and in which areas the United States' regulations are comparable to (or even ahead of) the GDPR.

II. BACKGROUND

A. United States Data Protection Laws

The United States' data protection laws are currently a patchwork collection of legislation that focuses primarily on certain areas of commerce and certain business types.[27] Aside from those areas and businesses, data protection has been a hands-off issue for Congress, though some recently proposed regulations demonstrate that some in Congress may be willing to take a more hardline approach to data protection.[28] The most applicable legislation to the Equifax data breach is the Fair Credit Reporting Act,[29] which regulates credit-reporting agencies, entities receiving credit reports, and entities furnishing information compiled in credit reports.[30] Further legislation protecting personal information includes the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[31] the Gramm-Leach-Bliley Act (GLBA),[32] and the Family Educational Rights and Privacy Act (FERPA).[33]

27. Ieuan Jolly, *Data protection in the United States: overview*, WESTLAW, https://1.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default (last visited Feb. 2, 2019). This article only examines regulations that govern private sector data protection. Regulations and instructions how government agencies are to protect their data are beyond the scope of this article.

28. *See infra* Section IV (Proposed Legislation Following the Equifax Breach).

29. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

30. *See id*.

31. Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160, 162, 164 (1996) (regulating health-related information transfers and storage).

32. Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2010) (regulating data protection of financial entities).

33. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974) (limiting the transfer of educational information).

B. European Union General Data Protection Regulation

The GDPR was approved by the European Union Parliament on April 14, 2016.[34] The GDPR declares the "right to protection of personal data" to be a fundamental right held by all natural persons.[35] As such, the protection granted by the GDPR is much more inclusive and comprehensive than U.S. law and reaches each and every entity that handles European Union citizen data whether located in the European Union or abroad.[36]

III. ANALYSIS AND COMPARISON

In general, the GDPR is a forward-looking attempt to protect data subject information and rights into the future.[37] A *data subject* is a singular person or company whose information is stored in a database or whose information was accessed from a database. As such, the GDPR speaks in general terms and does not speak of specific processes, risks, or mitigative strategies.[38] While the FCRA and HIPAA are both generalized in nature, neither statute encompasses the full range of protection afforded to individuals under the GDPR.[39]

As the GDPR is a far more comprehensive piece of legislation than its U.S. counterparts, this article will utilize the GDPR as a framework against which the United States laws will be compared due to their piecemeal nature. The GDPR begins regulating data protection prior to when the data subject provides their information to the covered entity[40]

34. *GDPR Portal: Site Overview*, EU GDPR.ORG, https://www.eugdpr.org/ [https://perma.cc/GRJ8-43EP].

35. General Data Protection Regulation, *supra* note 26, at art. 1(2).

36. General Data Protection Regulation, *supra* note 26, at art. 3.

37. General Data Protection Regulation, *supra* note 26, at art. 1(2).

38. *See generally* General Data Protection Regulation, *supra* note 26.

39. *See generally* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012); Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160, 162, 164 (1996).

40. "Covered Entity" refers to the business that stores a data subject's information and is regulated by the legislation being discussed. For the GDPR, covered entities include those storing, processing, or transferring data in the European Union as well as those storing, processing, or transferring data regarding data subjects who reside in the European Union or where European Union Member State laws apply. *See* General Data Protection Regulation, *supra* note 26, art. 3. For the FCRA, covered entities include credit reporting agencies, those receiving credit reports, and those furnishing information compiled in credit reports, each as defined in 15 U.S.C. § 1681(a). For HIPAA, covered entities include health plans, health care clearinghouses, business associates, and healthcare providers if they transmit health information electronically, each defined in 45 C.F.R. § 160.103. When other regulations are mentioned in this article, the article will explain who is considered a covered entity for the purposes of that regulation. For entities in the United States, it is imperative that the entity determine which U.S. regulations they must comply with, if any, before handling personal information.

and continues its regulation through the processing and storage stage until erasure of the protected information. Moreover, the GDPR regulates how breaches are to be handled.[41] In effect, there are six major areas addressed by the GDPR: (1) restrictions on collecting data and ensuring correct data; (2) restrictions on the processing of data; (3) restrictions on the transfer of data; (4) breach and unauthorized access prevention; (5) data subject notification and injury mitigation following a breach; and (6) covered entity oversight and liability.[42] This article will address each area individually.

A. Restrictions on Collecting Data and Ensuring Correct Data

While neither the GDPR nor U.S. legislation focus heavily on how data is collected initially, there are some limits in the GDPR that are currently unseen in U.S. legislation, some of which will be explored below. The GDPR allows data to be collected only for explicitly disclaimed and legitimate purposes, and the data must be limited to what is necessary for that purpose.[43] Additionally, the GDPR requires that each data subject consent to the storage of their personal data.[44] Furthermore, the GDPR allows for a data subject to revoke consent to storage or processing of their personal information,[45] though that revocation is not retroactive.[46] The GDPR data subject may also request that the covered entity erase their data (which is already required when the data is no longer necessary), consent to its withdrawal, or object to the data being stored or processed on the grounds of illegal data collection.[47]

41. *See generally* General Data Protection Regulation, *supra* note 26.

42. General Data Protection Regulation, *supra* note 26..

43. General Data Protection Regulation, *supra* note 26, at art. 5(1).

44. General Data Protection Regulation, *supra* note 26, at art. 7(1).

45. Personal information can simply be defined as the data subject's protected information stored by the covered entity. The exact information protected varies by legislation, with the GDPR being the broadest in its protections. The GDPR defines personal data as "any information relating to an identified or identifiable natural person.. . ." General Data Protection Regulation, *supra* note 26, art. 4(1). In a general sense, protected information is any information that could possibly be used to either identify the data subject or steal the data subject's identity. HIPAA, for example, limits protected data, or as the Act calls it, "individually identifiable health information," to that which either identifies the data subject or can be used to identify the data subject. 45 C.F.R. § 160.103 (1996). The FCRA, on the other hand, includes all information that has a bearing on the consumer's credit worthiness, their character, reputation, personal characteristics, and more. *See generally* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

46. General Data Protection Regulation, *supra* note 26, at art. 7(3).

47. General Data Protection Regulation, *supra* note 26, at art. 17(2). However, the covered entity is not required to erase the data if the covered entity is processing the data for: exercising "the right of freedom of expression and information;" complying with legal obligations; public health

The GDPR also places further restrictions on collecting certain types of data, including "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership . . . " and data regarding health or sexual orientation.[48] These types of data may only be collected under certain conditions.[49] Data regarding criminal convictions may only be collected and processed when controlled by an official authority or when authorized by European Union or Member State laws.[50]

Current U.S. law limiting data collection, much like U.S. data protection law in general, is a patchwork attempt to regulate data collection in certain areas. For medical information, HIPAA requires that the data subject be given an opportunity to object, though silence equals consent, to the covered entity storing the data subject's name, location in facility, condition, and other personal information in a directory—information which may be disclosed to those who ask for the data subject by name.[51] HIPAA defaults to allowing certain information to be stored, though there is a pretense of requiring consent.

There are two main reasons why there is little legislation that limits the data collection. First—for online data entry forms—the data subject has some level of discretion as to what information they will provide, if any. A data subject can refuse to supply information in many forms or to find another business who will store less information.[52] However, this option is non-existent when the covered entity collects data from someone other than the data subject, such as how credit reporting agencies collect information.

Second, if a covered entity stores information, it may be held liable for the damage caused by that information following a breach. By storing less information, it is possible for the entity to limit their potential damages following a breach because the hacker may not have enough information to cause high levels of monetary damages. For example, limiting the data stored solely to payment information could lead to damages of fraudulent transactions and costs of cancelling a credit card,

reasons; public interests or research archiving; or litigation. General Data Protection Regulation, *supra* note 26, art. 17(3).

48. General Data Protection Regulation, *supra* note 26, at art. 9(1).

49. General Data Protection Regulation, *supra* note 26, at art. 9(2) (allowing collection with explicit consent, if required or allowed under Member State law, or if other specific conditions are met).

50. General Data Protection Regulation, *supra* note 26, at art. 10 (stating that a database of criminal convictions may only be kept "under the control of official capacity.").

51. 45 C.F.R. § 164.510(a)(1) (1996).

52. A simple example is the consumer deciding to forego purchasing from a business that requires creating an account to checkout and finding a business that allows the consumer to check out as a guest.

while collecting information such as addresses, jobs, bank accounts, and other information collected by credit agencies could lead to damages resulting from identity theft.[53] As such, companies are incentivized to collect as little information as possible to complete their processing requirements or whatever they need the information for.

One further area of regulation contemplated by both the GDPR and U.S. law is how to ensure that an intermediary will provide accurate information about the data subject. This is one area in which U.S. laws, specifically the FCRA, are equal to or ahead of the GDPR to some degree. Credit agencies—the covered entities in the FCRA—get their information and compile credit reports primarily from information provided to the credit agency by businesses that have some relationship with the data subject.

The FCRA addresses furnishers of data (the intermediaries between the data subject and covered entity) by placing a duty upon the furnishers to provide accurate information as well as a duty to correct errors.[54] Additionally, if any information that the furnisher is providing to a credit agency is negative the furnisher must notify the data subject of the negative information and provide them with an opportunity to correct the data.[55]

The GDPR, FCRA, and HIPAA allow for data subjects to rectify any incorrect information that they notice, but it is at the data subject's initiative. The GDPR makes rectifying incorrect data a right held by the data subject which may be require the covered entity correct or complete their data.[56] The FCRA is slightly more restrictive when it comes to correcting discrepancies: the data subject may dispute information in their credit report, but the covered entity investigates and decides whether to change the information or not.[57] HIPAA grants the data subject the right to amend their health information, but the covered entity may deny the request under some circumstances.[58] The GDPR seems to grant a broader right of correction to the data subject, although it remains to be seen how the right to correction will be implemented in Europe.

The most promising direction in data collection limitations is the trend toward minimization. While the GDPR's data minimization laws are

53. *Compare, e.g.*, Hawkins, *supra* note 20 *with* Ramsey, *supra* note 6.

54. 15 U.S.C. § 1681s–2(a)(1)–(2) (2012).

55. 15 U.S.C. § 1681s–2(a)(7)(A)(i) (2012).

56. General Data Protection Regulation, *supra* note 26, at art. 16.

57. 15 U.S.C. § 1681i(a)(1), (a)(5) (2012).

58. 45 C.F.R. § 164.526(a) (1996) (allowing the entity to deny the request if: the covered entity did not create the data; the data "is not part of the designated record set;" the data is not available for inspection by the data subject; or the entity believes the data to be accurate and complete).

yet to be fully tested,[59] and the Consumer Privacy Protection Act's minimization requirement has not even been enacted, all data subjects would benefit from less data being stored about them. Most people have encountered forms for a loan, for a purchase, to sign up for any sort of service, or something else that made them ask, "What could they possibly need that information for?" Data minimization would either prevent that information from being requested or at least require an explanation for why the information is being requested.

B. Restrictions on Processing Data

Processing of data refers to how the collected data is to be used once collected. While the GDPR defines a *processor* separately as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller,"[60] a processor can also be the same entity that collects the data. If separate entities, the processor is limited to using the data only for the reasons that the collecting entity who contracted with the processor specified in the contract.[61] Processors are also held to the same standard as other covered entities under the GDPR in regard to breach notification, ensuring data subject rights, and fulfilling the requirements of the GDPR.[62] In essence, processors are treated almost identically to other covered entities under the GDPR, but the GDPR explicitly sets out processing as a separate stage of the data protection cycle and addresses it individually, requiring consent from a data subject for their data to be processed.[63]

Under the GDPR, the data subject must be informed of what information about them is to be collected, and how it will be utilized and processed prior to collection.[64] The data subject's consent must be "freely given, specific, informed and unambiguous.. . ."[65] If the protected information includes the special types of data discussed above,[66] any

59. The GDPR began enforcement on May 25, 2018. *See GDPR Portal: Site Overview*, *supra* note 36.

60. General Data Protection Regulation, *supra* note 26, at art. 4(8).

61. General Data Protection Regulation, *supra* note 26, at art. 32(4). The contract must set out how the data will be processed, transferred, kept confidential, kept secure. General Data Protection Regulation, *supra* note 26, art. 28(3)(a)–(d).

62. General Data Protection Regulation, *supra* note 26, at art. 28(3)(e)–(h).

63. General Data Protection Regulation, *supra* note 26, at art. 6(1).

64. General Data Protection Regulation, *supra* note 26, at art. 6(1) (explaining duties of a processor).

65. General Data Protection Regulation, *supra* note 26, at art. 4(11).

66. *See supra* Section III(A) (describing types of data that are more restricted than general information).

entity processing that data must keep a written record[67] of the processing, which may be accessed by the Supervisory Authority (to be discussed later in the article).[68]

The United States has no particular limits on processing under current law. Thankfully, data processing seems to be a mostly self-regulating area. Most people who have the option of choosing whether or not to provide their information have some idea about how the data will be used, if only by considering who is requesting the data. Processing limitations would be most helpful in circumstances in which the processing is not immediately obvious to the data subject, such as for further marketing, sale of information to other entities, or other less-obvious uses. In theory, processing limits and transparency would help to minimize the confusion from—and perhaps the occurrence of—spam emails or solicitation phone calls.

C. Restrictions on Transferring Data

In both European and United States law, a large part of the focus on data protection regulations regards transferring data. Blanket restrictions on data transfers would run the risk of stifling commerce, while complete allowance of data transfers without regulation would make it difficult to control who had access to personal information and how that information is spread to other entities. Data protection legislation must balance the needs of commerce, which benefits from open transfers of data, with the privacy and security needs of the data subject, who benefits from minimal data transfers.

The GDPR focuses mostly on the transfer of information outside the European Union to non-covered entities.[69] Because the GDPR covers all entities that store, process, or transfer data in the European Union, as well as those storing, processing, or transferring data regarding data subjects who reside in the European Union[70] or where European Union Member State laws apply,[71] all covered entities are held to the same standards. The GDPR ensures that any covered entity receiving a transfer of personal

67. The written record must include: contact information for the controller and the controller's data protection officer; the purpose of processing; a description of the types of data collected and the categories of data subject; types of recipients who the information will be disclosed to; any international transfers with safeguards taken; time limits for information erasure; and a general description of the covered entity's security measures. General Data Protection Regulation, *supra* note 26, at art. 30(1)–(4).

68. *See infra* Section III(F) (describing covered entity oversight agencies).

69. *See generally* General Data Protection Regulation, *supra* note 26.

70. General Data Protection Regulation, *supra* note 26, at art. 3(2).

71. General Data Protection Regulation, *supra* note 26, at art. 3(3).

information would have to possess the same level of security and follow the same regulations as the entity transferring the personal information. Thus, the GDPR sets two ways that a non-covered entity may receive a transfer of personal information from a covered entity: by adequacy decision[72] or by complying with appropriate safeguards.[73]

For an adequacy decision, the European Commission (Commission) must determine if the non-covered entity who is to be the recipient of the personal information meets the Commission's requirements for adequate protections.[74] If the non-covered entity meets the requirements promulgated by the European Commission, the transfer may take place without any authorization requirements.[75] Under the GDPR, the Commission must determine whether the non-covered entity's protections are adequate by taking into account the non-covered entity's respective national regulations ensuring data subject rights and data protection, including how data may be further transferred and how the data subject may redress issues with non-covered entity; the existence of independent supervisors over the non-covered entity and their enforcement powers; and the third country's or international organization's commitments to data security.[76] The Commission, upon deciding that protections are adequate, may then pass an act stating that the protections are adequate[77] and allowing transfers.[78] If the Commission has not issued an adequacy decision, data may only be transferred under the GDPR if the transferring entity has provided the appropriate safeguards and ensured that the data subject has appropriate remedies to guarantee access to their rights.[79] Safeguards may be provided by contract with public authorities, binding corporate rules, the use of standard data protection contract clauses approved by the Commission, or ensuring that all involved entities abide by approved codes of conduct paired with contractual obligations.[80]

The GDPR places further requirements on binding corporate rules that are used to demonstrate appropriate safeguards for a transfer to a non-covered receiving entity.[81] To be sufficient, the corporate rules must be

72. General Data Protection Regulation, *supra* note 26, at art. 45(1).
73. General Data Protection Regulation, *supra* note 26, at art. 46(1).
74. *See generally* General Data Protection Regulation, *supra* note 26, at art. 45.
75. General Data Protection Regulation, *supra* note 26, at art. 45(1).
76. General Data Protection Regulation, *supra* note 26, at art. 45(2).
77. General Data Protection Regulation, *supra* note 26, at art. 45(3).
78. General Data Protection Regulation, *supra* note 26, at art. 45(5-7) (stating that the act must be reviewed every four years and may be amended or repealed by the Commission).
79. General Data Protection Regulation, *supra* note 26, at art. 46(1).
80. General Data Protection Regulation, *supra* note 26, at art. 46(2).
81. *See* General Data Protection Regulation, *supra* note 26, at art. 47.

legally binding to every member of the corporation, give the data subject rights regarding the processing of their information, and specify certain information that would be accessible to the data subject.[82]

United States' regulations also place a significant emphasis on limiting transfers of information in several different regulations. The FCRA authorizes transfers of personal information in several situations by covered entities, though those situations are limited.[83] To protect the data subject in their employment, a covered entity may only supply a credit report to an employer if the employer certifies that they have complied with the FCRA, they have provided the data subject a summary of their rights, the data subject has been notified that a report may be obtained, and the data subject has consented to the disclosure to the employer in writing.[84] However, a covered entity may transfer a report on any consumer for credit and insurance transactions (even if the data subject did not initiate the transfer) if the data subject authorized the transfer, or if the transaction is a firm offer of credit or insurance; the

82. General Data Protection Regulation, *supra* note 26, at art. 47(1). The corporate rules must specify: (a) the structure and contact details of the corporation; (b) the data transfers to be made, including categories of information to be transferred, the type and purpose of processing, the category of data subject affected and the receiving entity; (c) the rules' "legally binding nature, both internally and externally;" (d) how data protection principles will be applied (data minimization, time limits for storage, how the GDPR requirements will be met, etc.); (e) the data subject's rights regarding processing and how rights are to be exercised (including the data subject's right to complain, obtain redress or compensation, and the data subject's right to opt out of decisions based solely on automated processing); (f) that the transferring party based in a Member State accepts liability for breaches of the corporate rules by the receiving entity; (g) how the data subject will be notified of the binding corporate rules; (h) what tasks the data protection officers or others are responsible for regarding monitoring and training for compliance; (i) the procedures a data subject must follow if they wish to file a complaint; (j) how the transferring entity will ensure that the receiving entity follows the binding corporate rules and how the results will be sent to the transferring entity's data protection officer and corporate board; (k) how the entities will report and record changes to the binding corporate rules and how the Supervisory Authority will be apprised of those changes; (l) how the entities will demonstrate compliance with the Supervisory Authority (particularly by making compliance reports available to the Supervisory Authority); (m) how the entities will report any legal requirements that may negatively affect the binding corporate rules to the Supervisory Authority; and (n) the "appropriate data protection training to personnel having permanent or regular access to personal data." General Data Protection Regulation, *supra* note 26, at art. 47(2).

83. 15 U.S.C. § 1681b(a) (2012). Transfers are authorized when the transfer is ordered by a court; when the data subject directs their information to be released; when the covered entity believes the information will be used for a credit transaction, employment, underwriting insurance, licensing requiring financial responsibility, valuations of existing credit obligations, or for legitimate business needs; to the government for issuing a credit card; to a child support agency; or to the Federal Deposit Insurance Corporation. *Id*.

84. 15 U.S.C. § 1681b(b)(1)–(2) (2012).

consumer has not opted out of the transfer; and the consumer is over the age of 21.[85]

Under HIPAA, transfers of health information are highly regulated.[86] The covered entity may transfer protected information to the data subject for treatment, payment, health care operations, or to others if the data subject consented to the transfer.[87] Covered entities may also transfer information: for the entity's own treatment of the data subject, the data subject's payments, or for healthcare operations; to other entities with a relationship with the data subject for healthcare operations or fraud protection; or to other entities in an organized health care arrangement for the health care arrangement's activities.[88] Covered entities are only required to disclose personal health information to the Secretary or when requested by the data subject.[89] In addition to covered entities, the business associates of the covered entities may only transfer personal health information under contract stipulations and only if the transfer does not violate the rules stated under HIPAA.[90] However, HIPAA is much like the GDPR in that it only protects identifiable information.[91] So long as the information transferred cannot possibly identify an individual data subject, the covered entity is not required to comply with the transfer requirements listed above, even if the non-identifying information is created from personally identifiable information.[92]

The GLBA applies to financial institutions and attempts to hold them responsible for protecting the privacy and personal information of their customers.[93] A financial institution may disclose personal information as needed to complete a transaction or maintain an account as authorized by the data subject; with consent of the data subject; to protect either the data subject or the entity from fraud; in order to mitigate risk; to those who possess a beneficiary interest in the data subject; to the data subject's

85. 15 U.S.C. § 1681b(c)(1) (2012). If the data subject did not authorize the transfer, the receiver may only receive the name and address of the data subject and any other information that does not demonstrate the relationship between the consumer and the creditor. 15 U.S.C. § 1681b(c)(2) (2012).

86. *See generally* 45 C.F.R. § 164.502 (1996).

87. 45 C.F.R. § 164.502(a)(1) (1996).

88. 45 C.F.R. § 164.506(a)–(c) (1996).

89. 45 C.F.R. § 164.502(a)(2) (1996). Secretary is defined by HIPAA to mean "the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated." 45 C.F.R. § 160.103 (1996).

90. 45 C.F.R. § 164.502(a)(3) (1996).

91. 45 C.F.R. § 164.502(d) (1996).

92. *Id.* (stating that covered entities do not have to comply with the disclosure requirements of 45 C.F.R. §164.502 if the information is not personally identifiable).

93. 15 U.S.C. § 6801(a) (2010).

fiduciary or representative; to insurance agencies; to those checking the entity for compliance; to the entity's attorneys, accountants, and auditors; to a consumer reporting agency; or in connection with transactions of a business if the transaction concerns the data subjects of the business.[94]

Finally, FERPA deals with the access to and accuracy of school records.[95] A covered entity under FERPA is an "educational agency or institution. . .which is the recipient of funds under any applicable [federal] program."[96] FERPA limits the transfers of education records of students (the data subject) by withholding federal funding to the covered entity if the entity transfers educational records to other entities without written consent of the data subject's parents.[97] FERPA also requires that the covered entity must keep a record for each data subject which contains a list of everyone who has requested or received access to the data subject's records and the interest that the accessor had.[98] That record is only accessible by the data subject, parents of the data subject, school officials responsible for the record, and auditors of the covered entity.[99]

United States laws place further requirements on receivers of transferred personal data. Under the FCRA, if the receiver of the personal data is taking negative action based on information provided by a covered entity, the receiver must notify the data subject of the negative action; provide the data subject's credit score to the data subject; provide the name of the covered entity providing the credit report; provide notice to the data subject of the data subject's right to a free copy of the credit report following the adverse action; and provide notice of the data subject's right to dispute the information in the report.[100] These requirements ensure that the data subject has an opportunity to redress the information that caused the negative action if possible. If the adverse action is based on information from a third party, the receiver must inform the data subject, upon the data subject's request, of the nature of the information the negative action was based on.[101] If the receiver of a credit report is using that report for solicitation, they must disclaim to the data subject that they have the right to prohibit information in their credit report from being used

94. 15 U.S.C. § 6802(e) (2010).
95. 20 U.S.C. § 1232g(a)(1)(A) (2006).
96. 20 U.S.C. § 1232g(a)(3) (2006).
97. 20 U.S.C. § 1232g(b)(1) (2006). The covered entity may transfer directory information without consent. *Id*.
98. 20 U.S.C. § 1232g(b)(4)(A) (2006).
99. *Id.* (explaining who may access the student's information).
100. 15 U.S.C. § 1681m(a) (2012).
101. 15 U.S.C. § 1681m(b) (2012).

for solicitation.[102] Similarly, receivers of information from an entity covered under HIPAA may only use the provided information in accordance with HIPAA and their contract with the covered entity, and the entity also must return or destroy the transferred information once its use is complete.[103]

Under the GLBA, a financial entity is not allowed to transfer any personal information unless the entity provides notice to the data subject in writing, the data subject has a chance to opt out of the transfer, and the data subject is informed how to opt out.[104] Finally, it is a violation of the GLBA to receive, attempt to receive, cause a transfer, or attempt to cause of transfer of another person's information by making a false statement or by providing a false document to an officer or agent of the financial entity.[105]

Much like other areas in the United States' data protection laws, laws that limit the transfer of personal information can either be restrictive or non-existent. For example, HIPAA and the GLBA, are highly restrictive of the personal information that can be transferred, while there are no data protection laws which prevent someone's internet-shopping history form being transferred to another entity for advertising purposes.

D. Breach and Unauthorized Access Prevention

As mentioned above, it is the criminal actions following a data breach that often bring about the damages suffered by individuals, whether through identity theft or fraudulent charges.[106] Hackers and those who obtain personal information for obviously nefarious purposes can be intimidating to victims because victims can assume that the hacker has no good intention for accessing their personal information.

The first step to preventing unauthorized access to personal information is to determine the risk of access attempts and what risks unauthorized access would pose to a data subject. Under the GDPR, a covered entity must determine the risk of a negative effect on the data subject's rights and freedoms caused by the entity's processing.[107] The

102. 15 U.S.C. § 1681m(d) (2012). The solicitor must also inform the data subject that the offer is only good while the data subject continues to meet the credit criteria, that the data subject has the right to have their name and address removed from the solicitor's list, and of the phone number to use to remove their name and address from the solicitor's list. *Id*.

103. 45 C.F.R. § 164.504(e)(2) (1996).

104. 15 U.S.C. § 6802(a)–(b) (2010).

105. 15 U.S.C. § 6821(a) (2010).

106. *See supra* Section I.

107. General Data Protection Regulation, *supra* note 26, at Art. 35(1).

covered entity must make that determination by consulting with their data protection officer prior to the start of information processing[108] and must reassess whenever there has been a change in processing.[109] The data protection impact assessment is particularly required when automated processing may produce a legal effect on a person,[110] the processing is large scale and involves the special types of information described above,[111] or includes a "systematic monitoring of a publicly accessible area on a large scale."[112]

A completed data protection impact assessment must contain the following: a description of processing operations and purposes; an assessment of proportionality and necessity in relation to the purposes of processing; an assessment of risks to the rights and freedoms of the data subject (including the right to privacy); and measures envisioned to address the risks identified.[113] If the data protection impact assessment determines a high risk to data subject rights before the implementation of mitigating actions, the covered entity must notify the Supervisory Authority before beginning processing,[114] who must provide written advice to the covered entity on how to protect data subject rights or forbid the processing entirely.[115] The notification must include the responsibilities of those doing the data processing, the purposes of the processing, the safeguards planned, contact information for the data protection officer, and a copy of the data protection impact assessment.[116] The covered entity must then take the steps necessary to comply with the Supervisory Authority's advice and must notify the Supervisory Authority of the steps taken to comply.[117]

United States data protection laws take a more generalized approach to breaches, sometimes considering a breach of a covered entity's database as an unauthorized transfer of personal information by the covered entity.[118] With the possibility of class-action lawsuits against

108. *Id.* (explaining the steps required for conducting a data protection risk assessment).

109. General Data Protection Regulation, *supra* note 26, at Art. 35(11).

110. The data subject may have the right to opt out of automated processing that produces a legal effect. *See* General Data Protection Regulation, *supra* note 26.

111. *See Supra* Section III(a) "Restrictions on collecting data and ensuring correct data."

112. General Data Protection Regulation *supra* note 26, at Art. 35(3).

113. General Data Protection Regulation *supra* note 26, at Art. 35(7).

114. General Data Protection Regulation, *supra* note 26, at Art. 36(1).

115. General Data Protection Regulation, *supra* note 26, at Art. 36(2).

116. General Data Protection Regulation, *supra* note 26, at Art. 36(3).

117. General Data Protection Regulation, *supra* note 26, at Art. 60(10).

118. *See e.g.* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x. 384 (6th Cir. 2016) (holding that Nationwide Insurance Company breached the FCRA by allowing unauthorized access to customer information).

entities for failure to prevent breaches, the majority of U.S. business's data protection comes from customer pressure.[119] HIPAA is the lone United States regulation that, on its face, requires covered entities to conduct an assessment of the risks to information confidentiality, integrity, and availability of protected health information.[120] Covered entities must then act upon that risk assessment by implementing security measures to reduce risks to a reasonable level, sanctioning employees who fail to satisfy the security policy requirements, and implementing ways to review data storage system activity.[121]

The second step to prevent unauthorized access is to take steps to mitigate the assessed risks. The GDPR requires that covered entities implement several types of policies and security steps to protect personal information. Generally, the covered entity must implement data protection policies where reasonable.[122] The GDPR requires covered entities to implement appropriate measures to ensure security appropriate to the risk, including pseudonymization or encryption of data; means to ensure continuing "confidentiality, integrity, availability and resilience of processing systems and services;" how a data subject may access their information following a breach; and a process for testing security.[123] More specifically, the GDPR requires that covered entities implement measures to safeguard personal information in order to protect data subjects' rights, which must ensure that only necessary information is processed and stored, and must ensure that personal information is not accessible to others without the data subject's actions.[124] Covered entities are also required to comply with Supervisory Authority opinions and decisions.[125] Supervisory Authority and Board decisions are both likely to be the best way to determine what protection is needed for covered entities to fulfill the GDPR requirements.

The FCRA requires that covered entities use reasonable procedures to avoid violations of the FCRA and to limit unauthorized transfers to only those purposes approved by the FCRA.[126] The procedures enacted by the covered entities must require users to identify themselves, certify how the

119. *See e.g.* James Jenkins, et al., v. Equifax Information Services LLC., No. 3:15-cv-004433-MHL. *See also e.g.* Remijas v. Neiman Marcus Grp., LLC., 794 F.3d 688 (7th Cir. 2015) (holding Neiman Marcus liable for a breach of its database in a class action suit).

120. 45 C.F.R. §164.308(a)(1) (1996).

121. *Id.* (listing steps required following a risk assessment).

122. General Data Protection Regulation, *supra* note 26, at Art. 24(2).

123. General Data Protection Regulation, *supra* note 26, at Art. 32(1).

124. General Data Protection Regulation, *supra* note 26 at Art. 25(1-2).

125. General Data Protection Regulation, *supra* note 26, at Art. 60(10).

126. 15 U.S.C. § 41 §1681e(a) (2012).

data will be used, and then ensure that the entity does not furnish a report that will be used in violation of the FCRA.[127] The FCRA also provides that "[f]ederal banking agencies, the National Credit Union Administration, the Federal Trade commission, the Commodity Futures Trading Commission, and the Securities and Exchange Commission shall" establish guidelines for financial institutions and creditors for identity theft, prescribe regulations to identify risks to data subjects, and prescribe regulations that would lessen the risk of identity theft or fraudulent charges.[128] It is these guidelines that create the U.S. policy and security requirements for financial institutions and creditors, rather than the FCRA on its face.[129]

HIPAA takes a different approach than the FCRA to policy and security requirements in that HIPAA requires a litany of procedures and safeguards to protect personal information. HIPAA requires that covered entities implement policies that minimize who can access protected information and for what reasons.[130] Entities are also required to limit requests to necessary information[131] and track access to information through the use of unique employee identification numbers.[132] Additionally, covered entities must "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations."[133] Entities must: "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information" that is transmitted, received, created, or maintained; protect against anticipated threats to security of information; protect against unpermitted uses; and ensure compliance by employees.[134] Finally, HIPAA requires that all policies be written[135] and reasonable based on weighing the size, complexity, and technical capabilities of the entity; the probability of risk; and the cost of the measures.[136] HIPAA's requirements, while significant, not only set the standard for U.S. data security but also sets requirements that may allow for breaches to be traced back to their origin and hopefully prevented in the future. While the FCRA and HIPAA take steps that are seemingly at

127. *Id.* (placing responsibility on the covered entity for how a transferee utilizes the data they receive).

128. Fair Credit Reporting Act, 15 U.S.C. § 41 §1681m(e)(1-2) (2012).

129. This article only examines the originating legislation. While agency regulations may create more demanding requirements, they are beyond the scope of this article.

130. 45 C.F.R. § 164.514(d)(1-2) (1996).

131. 45 C.F.R. § 164.514(d)(3) (1996).

132. 45 C.F.R. § 164.312(a)(2)(i) (1996).

133. 45 C.F.R. § 164.308(a)(1)(i) (1996).

134. 45 C.F.R. § 164.306(a) (1996).

135. 45 C.F.R. § 160.314(b)(1) (1996).

136. 45 C.F.R. § 164.306(b) (1996).

opposite ends of the spectrum to prevent breaches and unauthorized access, both options work to ensure that covered entities have some policy in place to protect personal information. The FCRA places the determination of what is required in the hands of political appointees,[137] while HIPAA explicitly requires certain policies of its covered entities.[138]

The GDPR puts into law what many businesses already do (or ought to do) once they decide that they need to store consumer data—even if data security seems to be common sense. From the smallest family business putting a lock on a file cabinet to the largest corporation encrypting their customers' data, risk identification and management is the key to surviving a lawsuit following a data breach.

E. Breach Notification and Injury Mitigation

A *data breach* is defined by the GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[139] More simply, a data breach is the unauthorized accessing of personal information, regardless of the steps taken following access.

The GDPR has comprehensive notification requirements following a data breach. Once a covered entity discovers a breach that is determined to result in a high risk to the data subject's rights and freedoms, the entity must notify affected data subjects without delay.[140] Notification of data subjects is not required if: the data accessed is unintelligible due to protective measures like encryption or pseudonymization; the entity's subsequent acts mitigate the risk to data subjects' rights and freedoms; or notification would take disproportionate effort, and the entity took an equally effective manner of notifying affected data subjects.[141] The

137. *See* 15 U.S.C. § 41 § 1681m(e)(1) (2012) (placing regulation prescribing power in the hands of "[f]ederal banking agencies, the National Credit Union Administration, the Federal Trade Commission, the Commodity Futures Trading Commission, and the Securities and Exchange Commission. . .").

138. *See e.g.* 45 C.F.R. § 164.514(d)(1-2) (1996); 45 C.F.R. § 164.514(d)(3) (1996); Health Insurance Portability and Accountability Act, 45 C.F.R. §164.312(a)(2)(i) (1996); Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.308(a)(1)(i) (1996); 45 C.F.R. § 164.306(a) (1996); 45 C.F.R. § 160.314(b)(1) (1996).

139. General Data Protection Regulation, *supra* note 26, at Art. 4(12)

140. General Data Protection Regulation, *supra* note 26, at Art. 34(1). The notification must be in clear, plain language and include name and contact information for the data protection officer, likely consequences of the data breach, and measures taken or proposed to address the breach. General Data Protection Regulation, *supra* note 26, at Art. 34(2).

141. General Data Protection Regulation, *supra* note 26, at Art. 34(3).

covered entity must also notify the Supervisory Authority of the breach within 72 hours of discovery[142] including the nature of the breach, what was accessed, contact information for the breached entity, consequences of the breach, and measures taken to mitigate damages.[143] The Supervisory Authority may then determine whether the criteria to make notification to the data subjects has been met.[144]

The FCRA does not in itself require notification to data subjects following breaches, but it does allow for the data subject to inform the covered entity that they may have been victim of identity theft.[145] HIPAA, however, requires that the covered entity notify the data subject within 60 days[146] if the entity believes that the data subject's information was "accessed, acquired, used, or disclosed as a result of such breach."[147] The HIPAA notification mirrors the notification required by the GDPR, requiring the circumstances of the breach, the information involved, the steps the data subject can take, what sort of mitigating actions the entity is taking, and who to contact for further information.[148]

Again, mirroring the GDPR, HIPAA requires that a covered entity must notify the Secretary of Health and Human Services of any data breach.[149] Additionally, and going beyond the GDPR requirements, HIPAA also requires notification to a state's media outlets if the breach affected more than 500 residents of that state and must include the same information required when notifying a data subject individually.[150] In addition to notifying affected data subjects and others following a breach, some regulations require additional steps to help mitigate the damages to data subjects. Of currently enacted regulations, only HIPAA requires that covered entities have a plan to mitigate damages and document any steps taken[151] while simultaneously protecting the accessed data from

142. General Data Protection Regulation, *supra* note 26, at Art. 33(1).

143. General Data Protection Regulation, *supra* note 26, at Art. 33(3).

144. General Data Protection Regulation, *supra* note 26, at Art. 34(4). (If the criteria for not requiring notification have not been met by the entity, the Supervisory Authority may require the entity to notify the affected data subjects.)

145. 15 U.S.C. § 41 § 1681c-2(b) (2012). The entity may issue a block following an investigation if the entity believes the block to be in good faith. 15 U.S.C. § 41 § 1681c-2(c) (2012).

146. 45 C.F.R. § 164.404(b) (1996).

147. 45 C.F.R. § 164.404(a) (1996). *See also* 42 U.S.C. 156 § 17932(a) (1996) (requiring that any entity that processes health information and discovers a breach must notify each data subject whose information was accessed).

148. 45 C.F.R. § 164.404(c-d) (1996).

149. 45 C.F.R. § 164.408(a) (1996).

150. 45 C.F.R. § 164.406(a-c) (1996).

151. 45 C.F.R. § 164.308(A)(7) (1996).

unauthorized destruction or alteration.[152] The GDPR, like in most aspects, has the most generally applicable requirements for notifications following breaches. Though HIPAA regulates the entities it covers, its reach is minimal when compared to the GDPR.

F. Covered Entity Oversight, Certification, and Liability

The GDPR creates four different levels of oversight for a covered entity: the entity's data protection officer,[153] the Supervisory Authority,[154] the Board,[155] and the European Commission.[156] The data protection officer, designated by the covered entity,[157] must have expert level knowledge in data protection,[158] must ensure that the entity complies with the GDPR and applicable laws, advise and monitor the data protection impact assessment, cooperate with the Supervisory Authority, and act as the Supervisory Authority's point of contact within the covered entity.[159]

The Supervisory Authority is an independent agency created by each European Union Member State to ensure consistent application of the GDPR by cooperating with the Board, European Commission, and other Supervisory Authorities.[160] The Supervisory Board's role is to determine what counts as a standard contractual clause for data transfers,[161] investigate covered entities for compliance,[162] correct the actions of covered entities,[163] advise covered entities and Member States,[164] and more.[165] The Supervisory Authority is also the point of contact for data subjects who wish to file a complaint about a covered entity for

152. 45 C.F.R. § 164.310(c)(1) (1996).

153. *See* General Data Protection Regulation, *supra* note 26, at Art. 37(3).

154. *See* General Data Protection Regulation, *supra* note 26, at Art. 51.

155. *See* General Data Protection Regulation, *supra* note 26, at Art. 68.

156. *See* General Data Protection Regulation, *supra* note 26, at Art. 92.

157. General Data Protection Regulation, *supra* note 26, at Art. 37(3).

158. General Data Protection Regulation, *supra* note 26, at Art. 37(5).

159. General Data Protection Regulation, *supra* note 26, at Art. 39(1).

160. General Data Protection Regulation, *supra* note 26, at Art. 51(1-2).

161. General Data Protection Regulation, *supra* note 26, at Art. 28(8).

162. General Data Protection Regulation, *supra* note 26, at Art. 58(1) (stating that the Supervisory Authority may audit entities, request information, review certifications, and access information and premises as needed).

163. General Data Protection Regulation, *supra* note 26, at Art. 58(2) (stating that the Supervisory Authority may warn or reprimand covered entities, order compliance, order breach notifications, restrict entity data processing or transfers, and impose fines).

164. General Data Protection Regulation, *supra* note 26, at Art. 58(3)(a-b).

165. *See* General Data Protection Regulation, *supra* note 26, at Art. 57 (listing enumerated powers of Supervisory Authorities); *See* General Data Protection Regulation, *supra* note 26, at Art. 58 (listing additional enumerated powers of Supervisory Authorities).

noncompliance, which the Supervisory Authority must investigate.[166] On an individual level, covered entities are kept in check by data subject complaints.[167]

The Board was created by the GDPR to be independent[168] and is composed of a chairperson, the European Union Data Protection Supervisor, and a representative of each head Supervisory Authority from each Member State.[169] The Board's role is primarily to settle disputes between Supervisory Authorities, advise the European Commission, and issue guidelines and best practices for covered entities.[170]

Finally, the European Commission is tasked with maintaining and updating the GDPR, subject to European Parliament and European Council objections.[171] The Commission must evaluate the GDPR every four years and submit proposals for amendments as needed.[172] If required for consistent data protection, the Commission may submit proposals to amend not only the GDPR, but also other European legislation.[173]

On the U.S. side, the FCRA is enforced by the Federal Trade Commission, which possesses "procedural, investigative, and enforcement powers . . . ."[174] HIPAA requires that a covered entity identify a "security official who is responsible for the development and implementation of the policies and procedures required"[175] and a contact person to receive complaints.[176] Entities under HIPAA answer to the Secretary of Health and Human Services, who receives and investigates complaints that include sufficient information.[177] Entities covered by the GLBA answer to agencies which create appropriate standards for

166. General Data Protection Regulation, *supra* note 26, at Art. 57.

167. General Data Protection Regulation, *supra* note 26, at Art. 77 (stating that a data subject may lodge a complaint to the Supervisory Authority holding jurisdiction over the data subject's residence, data subject's place of work, or to the Supervisory Authority with jurisdiction over the location of the alleged infringement).

168. General Data Protection Regulation, *supra* note 26, at Art. 69.

169. General Data Protection Regulation, *supra* note 26, at Art. 68(1-4).

170. General Data Protection Regulation, *supra* note 26, at Art. 70(1). The guidelines and best practices may cover breaches and breach notification; what counts as high risk to data subject rights and freedoms; criteria for data transfers; how the Supervisory Authorities should carry out their duties; how individuals should report violations of the GDPR; and how accreditation should occur. *See* General Data Protection Regulation, *supra* note 26, at Art. 70(1).

171. General Data Protection Regulation, *supra* note 26, at Art. 92(4).

172. General Data Protection Regulation, *supra* note 26, at Art. 92(2, 5).

173. General Data Protection Regulation, *supra* note 26, at Art. 98.

174. 15 U.S.C. § 41 § 1681s(a)(1) (2012).

175. 45 C.F.R. § 164.308(a)(2) (1996); *See also* 45 C.F.R. § 164.530(a)(1)(i) (1996).

176. 45 C.F.R. § 164.530(a)(1)(ii) (1996).

177. 45 C.F.R. § 160.306 (1996) (requiring name of subject of complaint, a description of the violation, is within 180 days of discovering the violation, and any other information prescribed by the Secretary).

financial institutions regarding the security and confidentiality of personal information, protections against threats to personal information, and requirements to protect against breaches.[178]

The GDPR incorporates a proverbial "carrot" for the entities it covers by offering certifications which entities may advertise to consumers.[179] Supervisory Authorities may create accredited certification bodies based on their independence and expertise,[180] who may certify a covered entity for up to three years[181] if the covered entity has met the minimum criteria for data protection, which may be demonstrated by providing information and access to the Supervisory Authority or certification body.[182] Any seal, marks, or signs denoting certification must be approved by the Board[183] and disseminated to the public along with an explanation of what the seal, mark, or sign represents.[184] It is these seals, signs, and marks that allow a covered entity to demonstrate its compliance with security standards to potential consumers, benefiting the business.

The GDPR also allows for certification of codes of conduct by Supervisory Authorities[185] that lay out how types of covered entities are to act.[186] The Board may set eligibility standards for bodies who will ensure code of conduct compliance,[187] and those bodies may be certified by Supervisory Authorities.[188] The Supervisory Authority with jurisdiction over the covered entity may revoke an entity's certification if the entity no longer meets the accreditation criteria or if the entity violates the GDPR.[189] No current U.S. legislation has an accreditation body or process.

178. 15 U.S.C. § 94 § 6801(b) (2010).

179. *See generally* General Data Protection Regulation, *supra* note 26, at Art. 41-42.

180. General Data Protection Regulation, *supra* note 26, at Art. 43(1-2).

181. General Data Protection Regulation, *supra* note 26, at Art. 41(7).

182. General Data Protection Regulation, *supra* note 26, at Art. 41(5-6).

183. General Data Protection Regulation, *supra* note 26, at Art. 42(1-3).

184. General Data Protection Regulation, *supra* note 26, at Art. 41(8).

185. General Data Protection Regulation, *supra* note 26, at Art. 40(5-6).

186. General Data Protection Regulation, *supra* note 26, at Art. 40(2) (stating that codes of conduct may regard: how processing is to be conducted; what are considered legitimate interests for processing; how data is to be collected and pseudonymized; what information is to be shared with the public and data subjects; how the data subject may exercise their rights; how minors' information will be handled; entity responsibilities to keep data secure; how notification following breaches should be handled; steps to transfer data to non-covered entities; and non-judicial resolutions for data subject-entity disputes).

187. General Data Protection Regulation, *supra* note 26, at Art. 41(3).

188. General Data Protection Regulation, *supra* note 26, at Art. 41(1-2) (stating that the certifying body must demonstrate independence, create procedures, assess code compliance by covered entities, create procedures to handle code violations and complaints, and not have a conflict of interest).

189. General Data Protection Regulation, *supra* note 26, at Art. 41(5).

The GDPR and U.S. laws also include a "stick" component by which covered entities are held liable for violations of differing degrees, both civilly and criminally. A Supervisory Authority may assess fines after considering the nature and character of the infringement, mitigating actions by the entity, responsibility of the entity, security measures taken by the entity, previous violations, how the Supervising Authority became aware of the violation, compliance with Supervisory Authority recommendations regarding the entity, adherence to codes of conduct or certification requirements, and other mitigating or aggravating factors.[190] A data subject who believes their rights have been infringed may sue any covered entity under the GDPR, the courts of the entity's Member State, or the Member State where the data subject resides.[191] Covered entities are liable to the data subject for any damages suffered for GDPR violations.[192]

Civilly, under the FCRA, a data subject may file suit in the appropriate district court for violations of the FCRA causing sufficient injury to the data subject.[193] Willful noncompliance with the FCRA makes a covered entity liable to the data subject for actual damages, punitive damages, court costs, and attorney fees.[194] Negligent noncompliance makes a covered entity liable to the data subject for actual damages, court costs, and attorney fees.[195] Additionally, anyone who fraudulently obtains personal information for an impermissible purpose may be liable to the FTC for damages.[196] Under HIPAA, if the Secretary of Health and Human Services finds noncompliance, a covered entity and its legal agents[197] may be liable to the Secretary for monetary penalties.[198] In short, under U.S. law, covered entities are liable monetarily for violations of their respective data protection regulations, either to the government or to the data subjects themselves.

190. General Data Protection Regulation, *supra* note 26, at Art. 83(2). The GDPR sets out limits for fines based on set limits or amount of business. *See generally* General Data Protection Regulation, *supra* note 26, at Art. 83.

191. General Data Protection Regulation, *supra* note 26, at Art. 79 (stating that entities that are public authorities acting under public powers may not be sued by data subjects).

192. General Data Protection Regulation, *supra* note 26, at Art. 82(1).

193. 15 U.S.C. § 41 § 1681p (2012).

194. 15 U.S.C. § 41 § 1681n(a) (2012).

195. 15 U.S.C. § 41 § 1681o(a) (2012).

196. 15 U.S.C. § 41 § 1681n(b) (2012).

197. 45 C.F.R. § 160.402 (1996).

198. 45 C.F.R. § 160.312 (1996). Monetary penalty amounts are to be determined by weighing the nature and extent of the violation, the number of data subjects affected, the temporal length of the violation, the injury caused, prior violations, and the financial condition of the violating entity. 45 C.F.R. § 160.408 (1996). Affirmative defenses are listed under 45 C.F.R. § 160.410 (1996).

Multiple U.S. regulations go beyond the GDPR and create criminal liabilities for violations. The FCRA makes knowingly or willfully obtaining personal information under false pretenses[199] or providing protected information to an unauthorized recipient[200] offenses that may require jail time. The GLBA makes it a violation to "obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person" by making a false statement or providing false documentation.[201] Violations of the GLBA may lead to fines or up to five years of imprisonment.[202]

The GDPR makes civil remedies more accessible to data subjects than most U.S. legislation, except for the FCRA. However, the U.S. regulations take a further step by criminalizing some violating actions. Imposing criminal liability is one of the few areas in which the United States is more stringent than the GDPR.

IV. PROPOSED LEGISLATION FOLLOWING THE EQUIFAX BREACH[203]

In the prior session of Congress, there were several bills introduced that attempted to improve current U.S. data protection laws. While discussing every bill that could possibly affect the data security field would likely be futile due to their numerosity, there are several bills that would make a substantial difference in the field of data security in the United States. Those bills include the Consumer Privacy Protection Act

199. 15 U.S.C. § 41 § 1681q (2012).

200. 15 U.S.C. § 41 § 1681r (2012).

201. 15 U.S.C. § 94 § 6821(a) (2010).

202. 15 U.S.C. § 94 § 6823(a) (2010). If the violator is violating other laws at the same time or has a pattern of violations involving more than $100,000 per year, the fines may be increased, and the violator may be jailed up to ten years. 15 U.S.C. § 94 § 6823(b) (2010).

203. The following examples of legislation did not make it past the committee stage. However, an overview of these proposals can offer valuable insight into potential steps that the United States may take in the future to bolster current data protection laws.

of 2017,[204] the Data Security and Breach Notification Act,[205] the Cyber Shield Act of 2017,[206] and the Consumer Data Protection Act.[207]

A. New Restrictions on Collecting Data and Ensuring Correct Data

The Consumer Privacy Protection Act of 2017 would have limited data collection much like the GDPR.[208] If passed, the Act would have required every covered entity to create a plan to minimize the amount of personal data stored by the entity and to minimize the time that the data is stored.[209]

B. New Restrictions on Processing Data

The Data Security and Breach Notification Act of 2017 would have required any covered entity that processes data to have a policy stating how the data will be maintained or used, the contact information for the security management officer, how vulnerabilities are determined and monitored, how the vulnerabilities will be mitigated, and how the data will be erased.[210] These policies could have possibly brought the U.S. onto equal footing with the GDPR.

C. New Regulation Regarding Breach and Unauthorized Access Prevention

The Consumer Privacy Protection Act of 2017 would have required covered entities to determine vulnerabilities and threats that could lead to unauthorized access, transfer, destruction, or use of personal information.[211] The entity would then have to determine the potential damages that may result from the vulnerabilities and threats and determine

204. Consumer Privacy Protection Act of 2017, S. 2124, 115th Cong. (1st Sess. 2017) (Sponsored by Senators Leahy, Markey, Blumenthal, Wyden, Franken, Baldwin, and Harris, introduced on November 14, 2017, and referred to the Committee on the Judiciary).

205. Data Security and Breach Notification Act, S. 2179, 115th Cong. (1st Sess. 2017) (Sponsored by Senators Nelson, Blumenthal, and Baldwin, introduced on November 30, 2017, and referred to the Committee on Commerce, Science, and Transportation).

206. Cyber Shield Act, S. 2020, 115th Cong. (1st Sess. 2017) (Sponsored by Senator Markey, introduced on October 26, 2017, and referred to the Committee on Commerce, Science, and Transportation).

207. Consumer Data Protection Act, S. 2188, 115th Cong. (1st Sess. 2017) (Sponsored by Senator Menendez, introduced on December 4, 2017, and referred to the Committee on Banking, Housing, and Urban Affairs).

208. S. 2124 § 202(a)(4)(c) (2017).

209. *Id.*

210. S. 2179 § 2(a)(1).

211. S. 2124 § 202(a)(3).

how sufficient their security precautions are likely to be.[212] Requiring pre-breach vulnerability minimization should, at the very least, make it easier for victims to prove a negligence claim.

Additionally, the Consumer Privacy Protection Act of 2017, which applies to any entity "engaging in interstate commerce that collects, uses, accesses, transmits, stores, or disposes of sensitive personally identifiable information in electronic or digital form of not less than 10,000 United States persons during any 12-month period,"[213] would require that a covered entity should implement a program that includes "administrative, technical, and physical safeguards" as appropriate to the entity to promote data subject privacy and data security.[214] The program required should protect against identified vulnerabilities by protecting against "unauthorized access, destruction, acquisition, disclosure, or use" of personal information.[215] Secondly, the Data Security and Breach Notification Act, applying to those not covered by the GLBA, the HITECH Act, or Title XI part C of the Social Security Act,[216] would require that entities have policies stating how data is to be collected, used, sold, maintained, and transferred as well as processes for preventing or mitigating identified vulnerabilities.[217]

If passed, the Consumer Privacy Protection Act of 2017 had the potential to bring U.S. data protection laws to a somewhat even level with the requirements of the GDPR. However, while the Data Security and Breach Notification Act improves data protection, it does not rise to the level of the GDPR.

D. Breach Notification and Injury Mitigation

Proposed U.S. data protection laws may require far more than the GDPR in notification and mitigation actions following a breach.[218] Multiple U.S. bills seem to be concerned with notifications following situations where breaches were not fully disclosed until well after

212. *Id*. (requiring a weighing of risks verses the preventative steps taken by the entity).

213. *Id*. § 201(b). The Consumer Privacy Protection Act of 2017 does not apply to financial institutions, HIPAA and HITECH regulated entities, or service providers. S. 2124 § 201(c).

214. *Id*. § 202(a)(1).

215. *Id*. § 202(a)(2).

216. *Id*. § 2(b)(1-2).

217. *Id*. § 2(a)(1) (2017).

218. *See generally* General Data Protection Regulation, *supra* note 26, *and compare* S. 2179, *with* S. 2124, *and* S. 2188.

discovery of a breach.[219] The Consumer Privacy Protection Act of 2017 would require that a covered entity who discovers a breach of their own database, a contracted party's database, or a service provider's database[220] notify any affected data subject[221] as soon as reasonably possible.[222] The Data Security and Breach Notification Act would require a covered entity to inform affected data subjects and the Federal Trade Commission of the breach,[223] if the entity believes there is a risk of unlawful conduct.[224] Finally, the Consumer Data Protection Act would require notification of the affected data subjects, the Federal Trade Commission, the Bureau of Consumer Financial Protection, and appropriate law enforcement agencies as determined by the Secretary of Homeland Security.[225]

Multiple regulations would have required mitigating actions following a breach. Requiring the least from the covered entity of the proposed legislations surveyed, the Data Security and Breach Notification Act requires that a covered entity must arrange for each affected data subject to receive free credit scores from a major credit agency following a breach.[226] Next, the Consumer Privacy Protection Act of 2017 would have required that covered entities provide five years of "identity theft prevention and mitigations services . . . to any individual notified . . . upon request of the individual and at no cost to the individual . . . ."[227] Most severely, the Consumer Data Protection Act would have required a covered entity to provide credit monitoring services for the data subject's lifetime at no charge to the data subject and that the entity create a fund to provide free assistance to data subjects who wish to dispute their records for the following ten years.[228]

219. *See e.g.* Ramsey, *supra* note 6 (stating that Equifax delayed admitting a breach), *and* Stemple, *supra* note 21 (stating that the full breadth of Yahoo's breach was not known until years later).

220. S. 2124 § 211(b).

221. *Id*. § 211(a). The notification must include the circumstances of the breach, the type of data accessed, mitigation acts taken, advice on steps the data subject can take, contact information for more information, and an offer for identity theft protection services if applicable. *Id.* § 214(a).

222. *Id*. § 211(c)(1).

223. S. 2179 § 3(a). The notification must include circumstances of the breach, categories of information accessed, contact information to learn more, a notice that the data subject may be able to get credit reports and how to do so, and contact information for identity theft information from the Federal Trade Commission. *Id*. § 3(d)(1)(B).

224. *Id*. § 3(g) (2017).

225. S. 2188, 115th Cong. § 2(b)(1)(A-B) (2017).

226. S. 2179 § 3(e)(1).

227. S. 2124 § 211(a). The service cannot be contingent upon the data subject agreeing to arbitration, as seen in the Equifax initial offer of identity theft protection. *See* Ramsey, *supra* note 6.

228. S. 2188 § 2(c)(3-4) (requiring also that the entity provide for credit freezes).

E. Covered Entity Oversight, Certification, and Liability

The Data Security and Breach Notification Act would have expanded the powers of the Federal Trade Commission to allow them to require covered entities under the FCRA to implement policies and procedures for the security and protection of personal information.[229]

The Cyber Shield Law of 2017 would have created a new program in order to certify products for certain levels of security.[230] If passed, the Secretary of Commerce would have been required to establish a Cyber Shield Advisory Committee[231] and appoint qualified members.[232] The Cyber Shield Advisory Committee would have been responsible for implementing a voluntary certification program for data security products,[233] maintaining a website that contains information about the products, along with a database of certified products, and information describing the benchmarks for the products and a description of the products.[234] The certifications would, in theory, allow for the same type of advertising and marketing opportunities afforded under GDPR certification.

The Consumer Privacy Protection Act of 2017 would have allowed for the Attorney General and the Federal Trade Commission to bring civil suits against entities violating the Consumer Privacy Protection Act.[235] The Data Security and Breach Notification Act would have redefined violations of the GLBA, treating them as "unfair and deceptive act[s] or practice[s] in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 USC 57a(a)(1)(B))"[236] and allowing for FTC enforcement action. Finally, the Consumer Data Protection Act would allow the FTC to bring civil suit against anyone who "negligently, knowingly, or willingly causes a data breach at a consumer reporting agency."[237] Data subjects would also be allowed to file civil suit against covered entities under the Consumer Data Protections Act.[238] The

229. S. 2179 § 2(a)(1).

230. *See* S. 2020, 115th Cong. § 5(a) (2017).

231. *Id*. § 3(a).

232. *Id*. § 3(c).

233. *Id*. § 4(a).

234. *Id*. § 5(a).

235. S. 2124, 115th Cong. § 203(a). State attorneys general are also authorized to sue violating entities. *Id*. § 204(a) (2017).

236. S. 2179, 115th Cong. § 55(c)(1-2) (2017).

237. S. 2188, 115th Cong. § 2(c)(1-2) (2017).

238. *Id*. § 2(c)(3)(B) (allowing suit against any person who "negligently, knowingly, or willingly caused a data breach at a consumer reporting agency in which the sensitive personal information of the affected individual was lost, stolen, or accessed without authorization").

Consumer Privacy Protection Act of 2017 would have concealment of a data breach resulting in injury of over $1,000 a criminal offense, punishable by fine or up to five years in jail.[239] The Data Security and Breach Notification Act would also have applied up to five years of jail time for concealing a breach that resulted in an injury of over $1,000.[240]

V. CONCLUSION

The GDPR is a comprehensive act that not only covers more entities within its jurisdiction,[241] but also holds those entities to an equal standard of security, regardless of the business's commercial mission, in order to protect the natural individual's right to protection of their personal data.[242] This level of comprehensiveness is unknown in the U.S. with the closest comparable regulation being HIPAA, in the author's opinion, due to its requirement of consent for storage of certain information,[243] its strong restrictions on data transfers,[244] its requirement of a risk assessment,[245] and its comprehensive notification requirements to data subjects,[246] media outlets,[247] and government entities.[248] HIPAA's main failing is that it covers too narrow a range of entities.

The proposed laws in the United States, specifically the Consumer Privacy Protection Act of 2017, have the chance to improve U.S. data protection laws to a comparable level with the GDPR. Primarily, the Consumer Privacy Protection Act of 2017 would apply not just to a specific field or a specific type of entity, but to any entity engaging in interstate commerce who deals with personal information on a significant level.[249] However, the Consumer Privacy Protection Act does exempt some entities, such as those who fall under the GLBA or HIPAA,[250] which would not completely resolve the piecemeal status of current U.S. data protection regulations.

Until the United States institutes a massive overhaul of its data protection regulation, it seems unlikely that entities not covered by the

239. S. 2124 § 101(a).
240. S. 2179 § 5(f)(1).
241. General Data Protection Regulation, *supra* note 26, at Art. 3.
242. General Data Protection Regulation, *supra* note 26, at Art. 1(2).
243. *See* 45 C.F.R. § 164.510 (1996).
244. *See* 45 C.F.R. § 164.502(a-c) (1996).
245. *See* 45 C.F.R. § 164.308(a)(1) (1996).
246. *See* 45 C.F.R. § 164.404(b) (1996).
247. *See* 45 C.F.R. § 164.406(a-c) (1996).
248. *See* 45 C.F.R. § 164.408(a) (1996).
249. *See* S. 2124, 115th Cong. § 201(b) (2017).
250. *See* S. 2124 § 201(c).

GDPR will be held to comparable standards. The U.S. laws as they currently stand not only neglect entire portions of the commercial market, but also neglect the opportunity to limit the data collected and ensure that appropriate safeguards are present to prevent breaches. Beyond voting with their wallet and dealing companies with better data protection when possible, the U.S.-based data subject has no recourse to ensure that the databases containing anything other than health information have sufficient safeguards. Sadly, in circumstances such as the Equifax breach, the data subject has no control over the information that is to be provided to the entity because the data subject has no personal relationship with the entity. The data subject's only personal recourse is a lawsuit following the data breach for the damages caused.[251]

251. Consumers are exercising their right to sue, and hundreds of lawsuits have been filed against Equifax since its breach in 2017. Hayley Tsukayama, *Equifax Faces Hundreds of Class-action Lawsuits and an SEC Subpoena Over the Way it Handled its Data Breach*, THE WASHINGTON POST (November 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/?utm_term=.b3dc1181fc61 [https://perma.cc/XW5U-9RC4].