Characterizing the Harms of Compromised Genetic Information for Article III Standing in Data Breach Litigation

TERRY WONG*

As direct-to-consumer genetic testing has proliferated, individuals face a heightened risk of having their genetic information exposed in data breaches. In response to these breaches, individuals that turn to the federal courts as an avenue for recovery must overcome the legal barriers that have often frustrated victims in traditional data breach contexts. In particular, these plaintiffs have struggled due to the circuit split among the U.S. courts of appeals over whether certain harms are sufficient to confer Article III standing in data breach cases. While federal courts continue to debate over the sufficiency of traditional data breach harms, compromises of genetic information raise exceptional considerations and harms that should favor the conferral of Article III standing.

This Note analyzes that the implications of data breaches involving compromised genetic information that justify an expansive approach to the conferral of Article III standing. Part II of this Note surveys the growing prevalence of data breaches and discusses the common legal obstacles that victims face in seeking recovery against breached entities. Part III outlines the relevant Article III standing requirements and reviews the circuit split among the U.S. courts of appeals by focusing on the primary hurdle for data breach victims — establishing injury in fact. Part IV raises and analyzes the

* Executive Managing Editor, Colum. J.L. & Soc Probs., 2019–2020. J.D. Candidate 2020, Columbia Law School. The author would like to thank Professor Clarisa Long for providing insightful guidance, and the staff of the *Columbia Journal of Law and Social Problems* for their thoughtful feedback and tireless editing.

exceptional features and implications of data breaches involving genetic information. In doing so, this Part characterizes the potential harms resulting from genetic information compromise and discusses how they should impact the Article III standing analysis to satisfy the injury-in-fact requirement.

I. INTRODUCTION

On June 4, 2018, MyHeritage — a genealogy company offering direct-to-consumer (DTC) genetic testing and family ancestry services — announced that it experienced a data breach exposing the email addresses and hashed passwords[1] of over 92 million users.[2] In a company statement, MyHeritage noted that it had no reason to believe that any other types of sensitive user information, such as "family trees and DNA data," had also been jeopardized and stolen as a result of the breach.[3] But what if it had? For DNA testing companies like MyHeritage, potential data breaches compromising genetic information raise serious, unique risks and implications regarding the privacy of consumers.

MyHeritage is a part of a rapidly growing industry of DTC genetic testing companies.[4] While genetic testing has traditionally

---

1. Password hashing is the process of converting passwords into a seemingly random string of characters that is designed to be extremely difficult to reverse. Andy Greenberg, *Hacker Lexicon: What Is Password Hashing?*, WIRED (June 8, 2016), https://www.wired.com/2016/06/hacker-lexicon-password-hashing [https://perma.cc/K4UX-H9M3]. It is often used as a security measure to protect data from being readable if compromised. *See id.* The ability of password hashing to protect the contents of data depends on the sophistication of the hashing scheme. *Id.* While strong password hashing could keep data secure in spite of a breach, some hashing schemes employed by commercial companies have proven to be ineffective. *See id.* For example, the data breaches of LinkedIn in 2012 and Ashley Madison in 2015 contained caches of hashed passwords that were subsequently cracked. *Id.*

2. *See* Admin, *MyHeritage Statement About a Cybersecurity Incident*, MYHERITAGE: BLOG (June 4, 2018), https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident [https://perma.cc/AKW3-FJHE].

3. *Id.* At the time of its 2018 data breach, MyHeritage only used DNA testing to provide ancestry services, but the company has since begun offering comprehensive health reports from this testing. *See MyHeritage Expands to Health; Launches New DNA Test Offering Powerful and Personalized Health Insights for Consumers*, BUSINESSWIRE (May 20, 2019), https://www.businesswire.com/news/home/20190520005426/en/MyHeritage-Expands-Health-Launches-New-DNA-Test [https://perma.cc/9FW6-XL3W].

4. Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECHNOLOGY REVIEW (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up [https://perma.cc/GCJ2-CNZ8]. After experiencing constant growth since the early 2000s, the DTC genetic testing industry more than doubled in 2017 — reaching a number higher than all previous years combined — and exceeded twelve million in 2018. *Id.* The U.S. market for DTC genetic testing was valued at over $299 million in 2018 and is expected to grow to $890 million by 2025. Sumant

been administered through healthcare providers, DTC genetic testing companies market directly to consumers, collect their DNA samples, and return test results through written or online reports.[5] These tests typically offer consumers the opportunity to learn information regarding family ancestry, common traits, and health predictions.[6] While genetic testing has traditionally been applied in numerous social, legal, and scientific contexts across society,[7] commercial testing companies have been able to amass large databases of genetic information that can be exploited for purposes such as drug development[8] and criminal investigation.[9] As the industry for commercial genetic testing continues to expand in the age of big data, questions arise over how private companies should be able to acquire, store, and use these massive troves of personal genetic information.[10]

Ugalmugale, *U.S. Direct-to-Consumer Genetic Testing Market Size by Test Type (Carrier Testing, Predictive Testing, Ancestry & Relationship Testing, Nutrigenomics Testing), by Technology (Targeted Analysis, Single Nucleotide Polymorphism (SNP) Chips, Whole Genome Sequencing (WGS)), Industry Analysis Report, Application Potential, Competitive Market Share & Forecast, 2019–2025*, GLOBAL MARKET INSIGHTS (Sept. 2019), https://www.gminsights.com/industry-analysis/us-direct-to-consumer-genetic-testing-market [https://perma.cc/SW7B-YBDD].

5. *See What Is Direct-to-Consumer Genetic Testing?*, NAT'L INSTS. OF HEALTH, NAT'L LIBRARY OF MED., GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/dtcgenetictesting/directtoconsumer [https://perma.cc/299S-KAL7] (last visited Mar. 29, 2020).

6. *Id.*

7. These uses have included establishing both criminality and exoneration, influencing reproductive choices, and much more. *See, e.g.*, *What Are the Types of Genetic Tests?*, NAT'L INSTS. OF HEALTH, NAT'L LIBRARY OF MED., GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/testing/uses [https://perma.cc/WB8M-9TBP] (last visited Mar. 29, 2020); *DNA's Revolutionary Role in Freeing the Innocent*, INNOCENCE PROJECT, https://www.innocenceproject.org/dna-revolutionary-role-freedom [https://perma.cc/8DW7-XT75] (last visited Mar. 29, 2020); Federica Cariati et al., *The Evolving Role of Genetic Tests in Reproductive Medicine*, 17 J. TRANSLATIONAL MED., Aug. 14, 2019, at 1, https://translational-medicine.biomedcentral.com/articles/10.1186/s12967-019-2019-8 [https://perma.cc/UD9C-QTGP].

8. *See* Antonio Regalado, *23andMe Sells Data for Drug Search*, MIT TECH. REV. (June 21, 2016), https://www.technologyreview.com/s/601506/23andme-sells-data-for-drug-search [https://perma.cc/8JYD-LKLN] (indicating that 23andMe has sold access to its genetic data to more than thirteen drug companies).

9. *See, e.g.*, Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Nov. 5, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [https://perma.cc/6R63-FD6G] (discussing the potential for law enforcement to access genetic information databases to further criminal investigations); Salvador Hernandez, *One of the Biggest At-Home DNA Testing Companies Is Working with the FBI*, BUZZFEED NEWS (Jan. 31, 2019), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy [https://perma.cc/57AA-JT8N].

10. As the DTC genetic testing industry reaches over twelve million people tested, *see* Regalado, *supra* note 4, advances in technology have allowed genomic sequences to be stored as permanent, electronic records that can be easily accessed, shared, and reproduced. *See*

While the aforementioned uses of genetic information have undeniable benefits, its extensive collection and storage in valuable commercial databases has created substantial, novel threats to personal privacy in part resulting from cybersecurity risks inherent to data storage. Not only will individuals be unable to fully control the use of their own genetic information, but it will also become subject to unauthorized third-party capture through data breaches. These risks and threats are exemplified by the persistent struggle of both public and private entities to secure their storages of aggregated user data against cyber threats.[11] Moreover, DTC genetic testing services have been subject to little regulation,[12] further raising concerns over consumer safety and protection. The increasing prevalence of DTC genetic testing by individual commercial entities creates large-scale caches of genetic information at risk of compromise through data breaches. Although MyHeritage was the first high-profile data breach of a DTC genetic information testing company, it is likely that there will continue to be others.[13]

In responding to these data breaches, the owners of the genetic information (or "data subjects")[14] have found themselves faced

---

Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Information Privacy Risks*, 27 HEALTH MATRIX 143, 148 (2017), https://scholarlycommons.law.case.edu/healthmatrix/vol27/iss1/8 [https://perma.cc/PKQ2-WAF8].

11. For example, cybersecurity incidents tripled between 2006 and 2013 in California and New York. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 946 (6th ed. 2018).

12. *See Regulation of Genetic Tests*, NAT'L INSTS. OF HEALTH, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/about-genomics/policy-issues/Regulation-of-Genetic-Tests [https://perma.cc/D5XE-NZJD] (last visited Mar. 24, 2020) ("As the field of genomics advances, genetic and genomic tests are becoming more common in, and out of, the clinic. Yet most genetic tests today are not regulated, meaning that they go to market without any independent analysis to verify the claims of the seller.").

13. As companies face around a thirty percent probability of experiencing a data breach involving a minimum of 10,000 records in the next two years, *see infra* Part II.A, there is little reason to think that the DTC genetic testing industry, valued at over $831 million with over twelve million consumers, *see* Regalado, *supra* note 4, would be immune from risk of data breaches.

14. This Note refers to the "owners" of genetic information as the individuals from which the genetic information was derived or originated. Also commonly known as the "data subjects," the "owners of genetic information" are the individuals who were the subjects of testing by the DTC genetic testing companies. Admittedly, the prevailing property theories maintain that the data is owned in the practical, commercial sense by the collectors, but these theories are increasingly disputed by other legal scholars, especially privacy advocates, evidenced by the rise in data privacy legislation among various states. This Note, however, refers to the data subjects as the "owners" of the compromised genetic information

with a serious threat for which they presently possess few avenues for protection and compensatory relief apart from litigation. The traditional route of bringing suit to recover over data breach harms, however, has proven to be a challenge for many plaintiffs seeking recovery in federal court due to the Constitution's Article III standing requirements. As a prerequisite to litigate in federal court, plaintiffs must have suffered a sufficient "injury in fact" that is fairly traceable to the challenged action of the defendant and likely redressable by a favorable court decision.[15] Unfortunately, plaintiffs seeking recovery over data breaches throughout various industries have struggled to meet these Article III standing requirements in many federal jurisdictions[16] due to challenges in adapting traditionally recognized legal doctrines to capture the harms resulting from the compromise and theft of consumer data.[17] Nonetheless, data breaches involving DTC genetic testing companies should raise unique considerations, thereby significantly impacting the relevant standing analysis and compelling federal courts to allow plaintiffs to overcome this traditional barrier.

This Note proposes that the novel implications of compromised genetic information justify an expansive approach to conferring standing to plaintiffs seeking recovery in the event of a DTC genetic testing company data breach. Part II surveys the prevalence of data breaches and the common obstacles that victims face in seeking recovery against breached service providers, such as adapting traditional common law doctrines to data breach harms. Part III outlines the relevant Article III standing requirements and focuses on the injury-in-fact prong as the primary hurdle for data breach victims attempting suit in federal court. This Part continues by discussing the circuit split among the U.S. courts of appeals over recognizing various theories of data breach harms. Part IV analyzes data breaches involving genetic information, including what makes genetic information different from traditional forms of information commonly exposed in other data breaches. In doing so, this Part also characterizes the unique resultant harms

---

because they are parties with the most diverse interests — namely, grounded in privacy — harmed in these data breaches and act as the plaintiffs in subsequent litigation.

15. *See* Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992)); *see also infra* Part III.

16. *See infra* Part III.B.

17. *See infra* Part II.B.

of compromised genetic information and how they impact the Article III standing analysis. Part V concludes that the unique and amplified harms of compromised genetic information should allow future plaintiffs seeking recovery over these data breaches to satisfy the injury-in-fact requirement for Article III standing.

II. THE CURRENT STATE OF DATA BREACH LITIGATION

To understand the implications of data breaches involving genetic information, it is beneficial to first examine the growing prevalence and impact of data breaches at large and to understand the barriers that have prevented past data breach victims from obtaining relief. Part II.A discusses the rapid rise in data breaches and identifies common types of consumer information that may subject individuals to harm when compromised. Part II.B then surveys the challenges of adapting traditional common law doctrines to the context of data breaches, which have frustrated attempts to characterize the harms for standing.

A. THE PREVALENCE OF DATA BREACHES

Over the past decade, data breaches have become increasingly common in the age of technology and big data.[18] The last few years have seen record highs in both the number of breaches and the number of records exposed, including 1632 data breaches in 2017 and over 446 million records exposed in 2018 containing various types of personally identifiable information (PII).[19] No major industry seems to have been immune to malicious data breaches and other similar cybersecurity threats, as large commercial companies, financial institutions, healthcare providers, and many other entities have been commonly targeted and hacked.[20] Furthermore, the risk of data breaches continues to rise, as one recent study showed that many companies face around a thirty percent

18. *See ITRC Breach Statistics 2005–2016*, IDENTITY THEFT RESOURCE CTR. (2017), https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf [https://perma.cc/S6XH-565E].

19. *See id.*; IDENTITY THEFT RESOURCE CTR., 2018 END-OF-YEAR DATA BREACH REPORT 9 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf [https://perma.cc/7DJH-AS2M].

20. *Id.*

probability of experiencing a data breach involving a minimum of 10,000 records in the next two years.[21]

In 2013, Yahoo! had all three billion of its accounts exposed, making it the largest known commercial breach in history,[22] and then it had the data of another 500 million of its users stolen in 2014.[23] In November 2018, Marriott International announced that it had suffered a multi-year data breach compromising the personal information of about 500 million customers.[24] These breaches were attributed to hackers who targeted customers and stole their information including names, physical addresses, phone numbers, dates of birth, email addresses, encrypted credit card details, travel histories, and passport numbers.[25] Data breaches of other large commercial entities, such as Equifax[26] and Anthem,[27] have also exposed additional types of information such as driver's license numbers,[28] Social Security Numbers (SSNs),[29] employment and income information,[30] and medical identifications.[31] The public sector has been similarly vulnerable, experiencing 443 government and military data breaches since 2014, which have amounted

---

21. IBM SEC. & PONEMON INST., 2019 COST OF A DATA BREACH REPORT 47 (2019). This amounted to a thirty-one percent increase in likelihood from 2014 to 2019. *Id.*

22. *See* Jonathan Stempel & Jim Finkle, *Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft*, REUTERS (Oct. 3, 2017), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1 [https://perma.cc/M73Q-ZBU4].

23. Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html [https://perma.cc/NS76-MQEC].

24. *See* Nicole Perlroth et al., *Marriott Hacking Exposes Data of up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html [https://perma.cc/R46N-E86X].

25. *See id.*; Vindu Goel, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/C4RV-R3UU]; Perlroth et al., *supra* note 24.

26. *See* Press Release, Fed. Trade Comm'n, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/8BV3-BWT8].

27. *See* Elizabeth Weise, *Massive Breach at Health Care Company Anthem Inc.*, USA TODAY (Feb. 5, 2015), https://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925 [https://perma.cc/TDA6-5JK3].

28. Nicole Perlroth & Cade Metz, *Equifax Breach: Two Executives Step Down as Investigation Continues*, N.Y. TIMES (Sept. 14, 2017), https://www.nytimes.com/2017/09/14/business/equifax-hack-what-we-know.html [https://perma.cc/9RDF-KU4V].

29. *Id.*

30. *See* Weise, *supra* note 27.

31. *Id.*

to over 168 million exposed records.[32] For example, the massive breach of the United States Office of Personnel Management in 2015 compromised the data of over four million current and former government workers.[33] This data breach involved the theft of information used for government security clearances, potentially including SSNs,[34] financial data, information on familial and romantic relationships, and record logs of meetings with foreigners.[35]

These data breaches have generated national attention and given rise to concerns over consumer privacy.[36] The loss of such large qualities and diverse forms of information in these breaches has resulted in serious harms to consumers over compromised personal information and substantial financial losses to the breached entities.[37] While entities collecting and storing large amounts of personal information often employ various technical security measures, such as encryption and de-identification, to protect individual privacy and the contents of data, these measures have been limited in effectiveness.[38] As such, personal privacy remains

---

32. *See* Paul Bischoff, *Government Breaches — Can You Trust the US Government with Your Data?*, COMPARITECH: VPN & PRIVACY (July 24, 2019), https://www.comparitech.com/blog/vpn-privacy/us-government-breaches [https://perma.cc/GU42-KP3M].

33. *See* David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. TIMES (June 4, 2015), https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html [https://perma.cc/5EET-3AC6].

34. *See id.*

35. *See* David E. Sanger et al., *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html [https://perma.cc/7MF2-GQFY].

36. *See, e.g.*, Karen Turner, *The Equifax Hacks Are a Case Study in Why We Need Better Data Breach Laws*, VOX (Sept. 14, 2017), https://www.vox.com/policy-and-politics/2017/9/13/16292014/equifax-credit-breach-hack-report-security [https://perma.cc/GJ4J-R63N].

37. The average cost of a data breach in the United States was $8.19 million — an average per record cost of $242. IBM SEC. & PONEMON INST., *supra* note 21, at 21, 22. These costs are the sum of expenditures associated with breach notification, detection and escalation, post data breach response, and lost business. *Id.* at 34. Lost business has consistently been the largest cost contributor, amounting to thirty-six percent of the total average cost in 2019. *Id.*

38. *See, e.g.*, Greenberg, *supra* note 1 and accompanying text (discussing password hashing); *see also* Fida K. Dankar et al., *The Development of Large-scale De-identified Biomedical Databases in the Age of Genomics — Principles and Challenges*, 12 HUM. GENOMICS, no. 19, Apr. 10, 2018, at 1–2, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5894154/pdf/40246_2018_Article_147.pdf [https://perma.cc/7UJR-HWCY] (examining the concerns and challenges surrounding deidentified biomedical databases, including the features of genomic data that make it difficult to deidentify); Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 SCIENCE 321, 321 (2013) (demonstrating that it was possible to re-identify research participants by cross-referencing genomic data from one database with free, publicly accessible Internet resources such as genealogical databases and public records).

seriously threatened by data breaches. The implications of these losses of information, however, differ significantly depending on the specific types of data involved and the industry of the breached entity.

The various harms experienced by data breach victims — as well as the chances of recovery over those harms — often center on the "sensitivity" of the exposed PII. Many types of traditional consumer information, such as much of those exposed in the Marriott breach (e.g., names, addresses, phone numbers, dates of birth, email addresses, and encrypted credit card details), may be generally be treated as less "sensitive" because of a relatively low risk of harm resulting from the loss of control over such information.[39] While the degrees of sensitivity of specific types of information, as well as the definition of "sensitive information" itself, is subject to some debate and interpretation, this Note treats these types of information as "non-sensitive." On the other hand, certain types of information that have the potential to result in serious, diverse harms when compromised are treated as more sensitive. The Yahoo! and Equifax breaches contain examples of more sensitive information being exposed — driver's license numbers, SSNs, employment and income information, and medical information.

As the prevalence of sensitive information often varies with the industry of the data collector, breaches in the healthcare and medical field[40] are especially concerning and relevant. This is due to

---

39. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133 (2015) ("[D]efinitions [of sensitive information] vary slightly, but all focus on a risk of harm resulting from a loss of control over information."). Many of these types of information are commonly given out or easily available to the public, making the risk of harm relatively low compared to social security numbers, for example, which often provide the basis for identify theft. *See Identity Theft*, USA.GOV, https://www.usa.gov/identity-theft [https://perma.cc/SV68-JB3P] (last visited Mar. 27, 2020).

40. Genetic testing is traditionally treated as a type of medical test, and thus commonly conducted in the healthcare and medical industry. *See What Is Direct-to-Consumer Genetic Testing?*, *supra* note 5. Commercial entities that provide DTC genetic testing, however, are not always categorized under the healthcare and medical industry. *See, e.g.*, IDENTITY THEFT RESOURCE CTR., *supra* note 19, at 108 (classifying MyHeritage's 2018 data breach under the category of "Business"). At the time of its 2018 data breach, MyHeritage was already providing DNA testing services but reported that its stored DNA data was not implicated in the breach. *See* Admin, *MyHeritage Statement About a Cybersecurity Incident*, MYHERITAGE BLOG (June 4, 2018), https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident [https://perma.cc/T67H-G4PX]. The Identify Theft Resource Center, which provides a comprehensive yearly report on data breach statistics, bases its "Medical/Healthcare" category on HIPAA's definitions of "covered entity" or "business associate," as well as including healthcare facilities and organizations which may be attached to schools and universities and some pharmaceutical manufacturers. *See* IDENTITY THEFT RESOURCE CTR., *supra* note 19, at 23. "Covered entities" are defined in the HIPAA

both the type of information implicated — typically labeled as "sensitive" — and the insight provided into the treatment of genetic information, which carries similar characteristics. The creation of specific federal legislation to protect personal information in the healthcare and medical fields exemplifies the worthiness of these types of information to have heightened protections. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established certain minimum protections and security procedures for the transfer of patient health information with violations enforced by the Department of Health and Human Services.[41] Similarly, the Genetic Information Nondiscrimination Act of 2008 (GINA) was created to "prohibit discrimination on the basis of genetic information with respect to health insurance and employment."[42]

Given that these types of information have been deemed worthy of heightened protections, it is also concerning that data breaches involving the healthcare and medical industries are occurring at a

---

rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. 45 C.F.R. § 160.103 (2013). A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. *Id.* As such, while HIPAA regulations were amended to include "genetic information" in the definition of "protected health information," DTC genetic testing companies are generally not regulated by the Act. *See id.*; *see also Genetic Information Privacy*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/genetic-information-privacy [https://perma.cc/2J9X-Z3QJ] (last visited Mar. 27, 2020) ("With genetic data — or any personal health information (PHI) — it's important to remember that HIPAA only applies to an organization if it is either a 'covered entity' or the business associate (BA) of one. Many non-covered entities collect genetic information, such as online genetic testing companies like 23andMe and genealogy websites like Ancestry.com.").

41. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); *see generally Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., HEALTH INFO. PRIVACY, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/U6L4-QMSL] (last visited Apr. 19, 2020). The Health Insurance Portability and Accountability Act protects the privacy of individually identifiable patient health information, referred to as "protected health information." 45 C.F.R. § 160.103.

42. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008). While GINA gives consumers a certain degree of protection by restricting health insurers and employers from discriminating against certain populations based on genetic data, it does not cover life insurance, long-term care insurance, or disability insurance, and does not prohibit health insurers from utilizing genetic results in determining insurance payments. Pascal Su, *Direct-to-Consumer Genetic Testing: A Comprehensive View*, 86 YALE J. BIOLOGY & MED. 359, 361 (2013). Additionally, beyond limiting the use of genetic information by health insurers and employers, GINA does not provide general privacy protections that would restrict DTC genetic testing companies from sharing confidential genetic information with third parties without consumers' consent. *See id.* at 361–62.

particularly high frequency. In one of the largest healthcare data breaches of 2018, UnityPoint Health exposed the information of 1.4 million patients in a phishing attack,[43] compromising health insurance information, dates of birth, medical history and diagnoses, treatment information, surgical information, prescriptions, payment information, driver's licenses, and other similar data.[44] As a whole, the healthcare and medical field experiences the second largest number of breaches and the highest rate of exposure.[45] Annual health data breaches have been on the rise, increasing seventy percent from 2010 to 2017, amounting to a total of 176.4 million records that were breached, lost, or stolen.[46] This has led some commentators to label data security in the healthcare sector as the "Wild West"[47] with worse protection than many other industries.[48] The high risk and frequency of these data breaches involving sensitive medical and healthcare information justifies a serious examination into the attendant harms and avenues by which victims may seek recovery. By considering the information implicated in these data breaches, as well as its treatment by legislatures and courts, this Note goes on to discuss how data breaches involving genetic information should be addressed.

B. COMMON OBSTACLES TO DATA BREACH LITIGATION

In response to the rapid increase in data breaches involving large amounts of personal information, affected individuals have

43. *See* IDENTITY THEFT RESOURCE CTR., *supra* note 19, at 8 (2019).

44. *See* Press Release, UnityPoint Health, Notice Regarding Security Incident (Jul. 30, 2018), https://www.unitypoint.org/filesimages/About/Security%20Substitute%20Notification.pdf# [https://perma.cc/NNA8-RHHF].

45. *See* IDENTITY THEFT RESOURCE CTR., *supra* note 19, at 2 (indicating that there was about a 187% increase in the number of records exposed in the medical and health care field from 2017 to 2018); *see also Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*, PONEMON INST. (May 12, 2016), https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1 [https://perma.cc/6A6A-NHYC] ("For the sixth year in a row, data breaches in healthcare are consistently high in terms of volume, frequency, impact, and cost. Nearly 90 percent of healthcare organizations represented in this study had a data breach in the past two years, and nearly half, or 45 percent, had more than five data breaches in the same time period.").

46. *See* Thomas H. McCoy Jr. & Roy H. Perlis, *Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010–2017*, 320 JAMA 1282, 1282 (2018).

47. Ifeoma Ajunwa, *Genetic Testing Meets Big Data: Tort and Contract Law Issues*, 75 OHIO ST. L.J. 1225, 1226 (2014).

48. *Id.* at 1226–27. A study showed that, compared to the finance, utilities, and retail industries, the healthcare industry had quantifiable differences in security performances, including the largest percent increase in security incidents and the slowest response times. *Id.*

flocked to federal courts in an attempt to gain relief and compensation for their data being exposed to unauthorized third-party capture. These attempts at recovery, however, have been met with mixed success due to a variety of burdensome obstacles to recovery. First, Part II.B.1 raises the preliminary challenge of finding and adapting the right traditional legal doctrine and entitlements under which to bring the data breach claims. Next, Part II.B.2 discusses how the traditional common law challenges will similarly apply to data breaches involving genetic information. Lastly, Part II.B.3 considers how the lack of legal solutions severely limits the ability of data breach victims to be made whole.

1. *Difficulties in Using Common Law Doctrines Following Traditional Data Breaches*

In responding to data breaches, consumers have often brought common law tort suits, alleging negligence, breach of contract, unjust enrichment, and others.[49] Tort law theories have been relatively successful compared to other common law doctrines for recovering from the harms of compromised information in data breaches. Nonetheless, they have still been frustrated by various barriers in adapting the traditional causes of action to the novel complexities of large-scale data breaches.

One prominent complicating factor preventing full and direct recovery over data breaches is that the most common perpetrators — i.e., the malicious attackers[50] — are typically unknown. In other words, these actors have no relationship or interactions with the consumers whose data was compromised following collection and

49. *See, e.g.*, *In re* SuperValu, Inc., 925 F.3d 955, 962 (8th Cir. 2019) (unjust enrichment, inter alia, under Illinois law); Resnick v. AvMed, Inc., 693 F.3d 1317, 1325 (11th Cir. 2012) (negligence per se and breach of fiduciary duty, inter alia, under Florida law); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010) (same under Washington law); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (negligence and breach of contract under Indiana law); *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1314 (N.D. Ga. 2019) (negligence under Georgia law); Reilly v. Ceridien Corp., No. CIV.A. 10-5142 JLL, 2011 WL 735512, at *2 (D.N.J. Feb. 22, 2011), *aff'd sub nom.*, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (breach of covenants of good faith and fair dealing, inter alia, under New Jersey law).

50. Data breaches are most commonly caused by malicious attacks, a trend that has been increasing in recent years. *See* IBM SEC. & PONEMON INST., *supra* note 21, at 6 ("Malicious attacks were the most common and most expensive root cause of breaches[.] The study found that data breaches originating from a malicious cyber attack were not only the most common of the breaches studied, but also the most expensive. Since 2014, the share of breaches caused by malicious attacks surged by 21 percent, growing from 42 percent of breaches in 2014 to 51 percent of breaches in 2019.").

storage by commercial entities. This leaves plaintiffs with the difficult and complex task of framing their harms against the service providers and entities storing or processing their data, as opposed to a more blameworthy malicious actor. This framing — often as a negligent failure to adequately safeguard the data — requires an examination into the duties owed by the service providers to the subjects of the compromised personal identifiable information and the damages that may be inferred over the fact that the breach occurred.

In framing their injuries towards service providers, plaintiffs have attempted to adapt traditional tort duties to the context of data breaches with mixed results. Recently, some plaintiffs have been successful with claims of negligence (in inadequately safeguarding or improperly disclosing consumer PII), amounting to harms such as identity theft. Other courts, however, have been very reluctant to accept these theories of harm.[51] This challenge has even generated scholarship calling for new, specific causes of action in tort for data breaches.[52] Despite the challenges, victims continue to bring claims over data breaches in tort law in order to push forward the developing case law. This seems partly due to the alternative avenues of relief in common law, such as contract law and property law, containing even greater legal barriers to be effective for plaintiffs.

Contract law has not proven to be a more viable alternative for protection and recovery because plaintiffs attempting to bring these claims have been met with substantial difficulties such as a lack of explicit terms covering liability for data breach harms. First off, plaintiffs typically have no opportunity to bring contract claims against the primary malicious actors — i.e., hackers that commit the data breaches and theft — due to the issue of attribution and the lack of a contractual relationship. Again, data breach victims are forced to attempt recovery against the service providers with whom they contracted, instead of the party that gained unauthorized access to the data. This approach of assigning liability to service providers, however, is often frustrated by complex terms of service agreements that users are required to accept, and

51. In federal cases, the rejection of these theories has largely occurred through requirement of Article III standing. *See infra* Part III.

52. *See* Ajunwa, *supra* note 47, at 1257–61.

which often do not contain provisions regarding redress for inadvertent disclosures of user information.[53]

Additionally, property law has similarly proved insufficient as a viable avenue for recovery because data breach victims have generally been found to lack property rights to the implicated personal data. In just the occurrence of information being exposed, data breach victims are not deprived of the use of any physical property. Possible property rights in personal data would instead be over intangible assets more akin to intellectual property rights. While entitlements to intellectual property revolve around giving exclusive rights of control to put intangible ideas into tangible forms for consumption, property rights have not been assigned to PII to allow individuals from whom the information originates to control their use and distribution. Some scholars have nonetheless argued for property-based models for consumers to maintain stakes in their personal information and the data pools that companies aggregate.[54] This would allow the consumers, as the subjects or generators of individual pieces of data, to claim a level of control or compensation over their data.[55] Any such compensation, however, would likely be negligible and difficult to establish as the value of big data is typically in the aggregation and subsequent processing, not the individual pieces that consumers contribute. As the development of property rights for individuals seeking to control their PII is hindered by these considerations, tort law and privacy rights continue to be the more prominent avenue for recovery.

2. *Challenge of Adapting Common Law Doctrines to Genetic Data Breaches*

The common law challenges faced by plaintiffs attempting to recover from traditional data breaches are largely no different regarding data breaches involving genetic information. For the reasons mentioned above, common law causes of action to recover

53. *See id.* at 1233–34 ("Despite what should be widespread knowledge about the insecurity of online information, a survey of twenty-two genetic testing companies, which provide the results of genetic testing online revealed something surprising: all of the companies' agreements neglect to include a provision regarding the redress of inadvertent disclosures of the information entrusted to them.").

54. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2095–116 (2004).

55. *See* Max N. Helveston, *Reining in Commercial Exploitation of Consumer Data*, 123 PENN ST. L. REV. 667, 690 (2019) (discussing the "pseudo-property rights" that legislation like the California Consumer Privacy Act provides to consumers).

from compromised genetic information will similarly find the greatest success in tort law, as opposed to the other doctrines. Contract claims against DTC genetic testing companies will likely be impeded by exculpations of liability or insufficient consumer information protections in terms of service. Property claims over compromised genetic information will be treated similarly to those involving other types of information traditionally targeted in data breaches. In particular, property theories are difficult to sustain in attempts at data breach recovery because in most instances, including with DTC genetic testing companies, users voluntarily hand over their personal information without maintaining individual rights of control. Some commentators have argued that personal genetic information contains qualities unlike other forms of PII, possibly justifying an exception to the general finding of no individual rights over personal data.[56] This notion is commonly referred to as "genetic exceptionalism."[57] These arguments are grounded in the characteristics of genetic information that make it unique from other types of personal data and are discussed below.[58] While genetic information may have a stronger argument for the conferral of individual property rights, the general and consistent denial of such rights over consumer-generated data renders property law an unlikely avenue by which these data breach victims can seek recovery.

On the other hand, tort law causes of action, such as in negligence or invasion of privacy, will continue to serve as the most prominent avenue for recovery for individuals victimized by data breaches compromising personal information. Genetic information will not only implicate the heightened treatment given to health information but should also justify even greater protection and depth in establishing the harms of compromise.[59] That being

56. *See* Samual A. Garner & Jiyeon Kim, *The Privacy Risks of Direct-to-Consumer Genetic Testing: A Case Study of 23andme and Ancestry*, 96 WASH. U. L. REV. 1219, 1241 (2019) ("[S]everal important features of genetic information strongly support genetic exceptionalism: familial nature, predictive ability, function as a unique identifier, stability and immutability, and potential for discrimination and stigmatization based on genetic information.").

57. *Id.*

58. *See* Benjamin E. Berkman, *Refuting the Right Not to Know*, 19 J. HEALTH CARE L. & POL'Y 1, 68 (2016). This characteristic is discussed further in this Note. *See infra* Part IV.A.

59. The justifications for treating genetic information with greater care than the already heightened current treatment of health and medical information are discussed below. *See infra* Part IV.A.

said, the need to adapt current causes of action or adopt new ones to protect disclosed genetic information remains.

3. *Lack of Legal Solutions*

Not only have plaintiffs struggled to adapt traditional common law doctrines to the complexities of data breaches for effective relief, but Congress has also failed to pass any substantial, comprehensive federal law protecting consumers from modern data breach harms. Instead, information privacy protections are clustered and sectored throughout different, unrelated legislation which do not provide private causes of action.[60] As legal doctrines slowly evolve to address data breach harms and their attendant legal issues, legislation related to data breaches has primarily focused only on breach notification.[61] By now, every state in the U.S. has requirements stating that companies experiencing commercial data breaches must report occurrences to customers within a set amount of hours.[62] These protections stopping at notification, however, do not provide consumers with an adequate remedy to the harms from compromised information.

Due to the large-scale nature of many data breaches, often resulting in the information disclosure of millions of consumers nationwide, class actions in federal court are typically a highly desired and appropriate avenue for victims to bring suit. These plaintiffs, however, face substantial problems trying to stay in

---

60. *See, e.g.*, Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681–728 (codified at 15 U.S.C. §§ 6501–6506) (providing enforcement by states' attorneys general under § 6504 and the Federal Trade Commission under § 6505); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. § 6805) (providing enforcement of HIPAA by the "Bureau of Consumer Financial Protection, the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission. . . ."); Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320d-5–d-6 (defining terms and enforcement protocols that specifically limit enforcement actions to the Department of Health and Human Services and individual states' attorneys general); *see also* Dunmire v. Morgan Stanley DW, Inc., 475 F.3d 956, 960 (8th Cir. 2007) (collecting cases indicating that no private right of action exists for violations of the Act); Lee-Thomas v. LabCorp, 316 F. Supp. 3d 471, 474 (D.D.C. 2018) (collecting cases indicating that circuits have reached a consensus that the statutory language of HIPAA grants no private right of action).

61. *See* SOLOVE & SCHWARTZ , *supra* note 11, at 945.

62. *See Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 29, 2018), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/SA56-Y2M4] ("All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.").

federal court for their claims to proceed on the merits. The primary problem, which often frustrates the success of substantive tort law claims, is establishing the harms — and causation — suffered by individuals from compromised information in data breaches. This barrier is embodied in the Article III constitutional requirements, which establish that plaintiffs must first minimally allege sufficiently cognizable injuries, even before attempting to satisfy or adapt legal doctrines to justify relief from the court.

This preliminary step has proven difficult for many plaintiffs seeking recovery over data breaches and is the focus of this Note in the following Part. The failure to establish harms beyond those deemed too indirect or intangible has served to be a substantial obstacle to data breach litigation, resulting in many cases being thrown out for lack of Article III standing. More conservative circuits have drawn from other legal doctrines and legislative treatment (or rather lack thereof) of data breach harms to conclude that the harms are too speculative, hypothetical, or inchoate to allow the suits to proceed.[63] Other federal jurisdictions, however, have been more liberal in acknowledging data breach harms such as heightened risks of future injury and have taken a favorable, expansive approach to standing.[64]

III. ARTICLE III STANDING FOR DATA BREACH CASES

Many attempts to recover for data breaches have been stopped for failure to establish Article III standing to litigate in federal court. The U.S. Constitution's Article III standing requirements are based on the principle of separation of powers and ensure that federal courts only resolve "cases" and "controversies" that are of the justiciable sort referred to in Article III.[65] To satisfy this case-or-controversy limitation on federal judicial authority, the federal court must find that: (1) the plaintiff(s) suffered an "injury in fact" that is "concrete and particularized and actual or imminent, not conjectural or hypothetical"; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a

63. *See infra* Part III.B.2.
64. *See infra* Part III.B.1.
65. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

favorable decision.[66] As the party invoking federal jurisdiction, the plaintiff bears the burden of establishing these elements.[67] Furthermore, at the pleading stage, the plaintiff must clearly allege facts demonstrating each one.[68] Due to the substantial difficulties in characterizing data breach harms through various common law theories, the injury-in-fact requirement is particularly burdensome for data breach victims seeking recovery.

A. THE "INJURY IN FACT" REQUIREMENT

While the plaintiff must establish all three elements for Article III standing, the injury-in-fact requirement is arguably the most substantial obstacle for data breach cases. This is partly because injury in fact is the "[f]irst and foremost" element for standing.[69] One of the most difficult tasks for plaintiffs has been characterizing data breach harms in ways that sufficiently establish injury in fact. This inquiry has resulted in a circuit split among the U.S. courts of appeals, with many jurisdictions declining to acknowledge the sufficiency of data breach harms for Article III standing.[70] This Note focuses on the injury-in-fact requirement and how its analysis is impacted by data breaches involving genetic information.

The injury-in-fact requirement in data breach cases is essential for ensuring that the following question is answered in the affirmative: is a victim whose information is compromised worse off than before?[71] Establishing injury in fact requires the plaintiff to show that an invasion of a legally protected interest is "concrete and particularized, and actual or imminent, not conjectural or hypothetical.[72] These elements are discussed in this order, beginning with an explanation of a concrete and particularized protected interest.

---

66. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000) (citing *Lujan*, 504 U.S. at 560–61).

67. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (citing FW/PBS, Inc. v. City of Dallas, 493 U.S. 215, 231 (1990)).

68. *Id.* (citing Warth v. Seldin, 422 U.S. 490, 518 (1975)).

69. *Id.* (quoting Steel Co. v. Citizens for Better Environment, 523 U.S. 83, 103 (1998)).

70. Discussed below in Part III.B.2.

71. *See* SOLOVE & SCHWARTZ, *supra* note 11, at 960.

72. *Spokeo*, 136 S. Ct. at 1548 (internal quotation marks omitted) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

1. *The Harm Must Be "Concrete and Particularized"*

The first requirement to establish injury in fact contains two necessary and distinct elements: the harm must be both "concrete" and "particularized."[73] A "particularized" injury must affect the plaintiff in a "personal and individual way."[74] A plaintiff can satisfy particularization by alleging a personal injury, actual or threatened,[75] such as by describing how one's personal interests are individualized and not collective or alleging a violation of one's own statutory rights.[76]

As a distinct requirement from particularization, a "concrete" injury must be one that actually exists, conveying the usual meaning of being "real" and not "abstract."[77] In discussing how the dissemination of information online could amount to sufficient harms, the Supreme Court in *Spokeo, Inc. v. Robins* specifically pointed out that, while tangible injuries may be easier to recognize, intangible injuries can also be concrete.[78] In determining whether intangible harms rise to the level of injury in fact, the Court stated that "both history and the judgment of Congress play important roles."[79] History can be particularly instructive if the "alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[80] Congress can also help elevate intangible injuries by conferring statutory rights.[81] This discussion is particularly important for data breach cases, as the concreteness of the injuries is often strongly challenged.

Often a focus in data breach cases, the risk of real harm can also be sufficient for establishing injury in fact.[82] This is exemplified by a long history of tort cases allowing recovery for harms that

---

73. *Id.* at 1548–49.
74. Lujan v. Defenders of Wildlife, 504 U.S. 555, 559 n.1 (1992).
75. *See Spokeo*, 136 S. Ct. at 1548 (collecting cases).
76. *See id.*
77. *Id.* (citing BLACK'S LAW DICTIONARY 479 (9th ed. 2009); WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 472 (1971); RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 305 (1967)).
78. *Id.* at 1549 (citing two examples of cases involving intangible injuries that are nonetheless concrete: Pleasant Grove City v. Summum, 555 U.S. 460 (2009) (free speech); Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520 (1993) (free exercise)).
79. *Id.*
80. *Id.* (citing Vermont Agency of Natural Resources v. United States *ex rel.* Stevens, 529 U.S. 765, 775–77 (2000)).
81. *Id.* (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992)).
82. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013).

may be difficult to prove or measure.[83] That being said, the Court in *Spokeo* made sure to distinguish between cases that entail a sufficient degree of risk and "bare procedural violation[s]."[84]

2. *The Harm Must Be "Actual or Imminent"*

The second requirement to establish injury in fact is that the plaintiff must have suffered an invasion of a legally protected interest which is "actual or imminent, not conjectural or hypothetical."[85] This element ensures that the "alleged injury is not too speculative for Article III purposes — that the injury is 'certainly impending'"[86] — as allegations of possible future injury are not sufficient.[87] As the concept of imminence is somewhat elastic, the inquiry for this element often focuses on establishing the breaking point of stretching beyond what is allowed for injury in fact.[88] Clearly outside of sufficient imminence is where the plaintiff "alleges only an injury at some indefinite future time, and the acts necessary to make the injury happen are at least partly within the plaintiff's own control."[89] This requirement ensures that a case is not decided in which no injury actually occurred. The precise extent of imminence, however, does not need to be established.[90] The "imminent" element is particularly important Article III standing in data breach cases because some of the proposed harms are centered around what an unknown third-party will do with the personal data that was accessed without authorization.

In *Clapper v. Amnesty International*, the Supreme Court addressed how speculative harm should be analyzed for purposes of the "actual or imminent" requirement of injury in fact for Article III standing.[91] Here, the Court rejected the Second Circuit's "objectively reasonable likelihood" standard for assessing whether the

83. *Spokeo*, 136 S. Ct. at 1549 (citing RESTATEMENT (FIRST) OF TORTS §§ 569 (libel), 570 (slander per se) (AM. LAW INST. 1938)).

84. *Id.* at 1550.

85. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (internal citations omitted).

86. *Id.* at 555, 564 n.2.

87. *See Clapper*, 568 U.S. at 409 (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). Additional cases discussing this component include DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 345 (2006); Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 190 (2000); *Lujan*, 504 U.S. at 565 n.2, 567 n.3 (1992); Babbitt v. Farm Workers, 442 U.S. 289, 298 (1979).

88. *See Lujan*, 504 U.S. at 564 n.2.

89. *Id.*

90. *Id.*

91. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).

future, speculative harm was sufficient for injury in fact.[92] In this case, the plaintiffs based their claims of injury on the likelihood that the United States would unlawfully intercept their communications with foreign contacts in violation of section 1881a of the Foreign Intelligence Surveillance Act.[93] In rejecting the plaintiff's theories, the Court found that the "highly speculative fear" relied on a "highly attenuated chain of possibilities" that could not be certainly impending to satisfy the requirement of imminence.[94] In supporting this reasoning, the Court also specifically noted the absence of evidence of actual harm, as well as the lack of allegations that the Government had taken steps towards carrying out the acts that would result in actual harm — i.e., whether the Government had sought court approval for communications surveillance.[95]

Acknowledging a "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors," the Supreme Court has concluded that allegations of future injury may suffice if the threatened injury is "certainly impending," or there is a "'substantial risk' that the harm will occur."[96] Moreover, while a substantial risk of future harm, which may "prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," can be sufficient for imminence, the Court added that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[97] As such, data breach victims seeking to recover in federal court must sufficiently allege harms that have already occurred or risks of injury that are highly

92. *Id.*

93. *Id.*; 50 U.S.C. § 1881a (2012).

94. *Clapper*, 568 U.S. at 410 (listing the following premises that were required for the plaintiff's argument of highly speculative fear: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts). *See also* Summers v. Earth Island Inst., 555 U.S. 488, 496 (2009) (standing theory rejected for having overly speculative chains of possibilities); Whitmore v. Arkansas, 495 U.S. 149, 157–60 (1990) (same).

95. *Clapper*, 568 U.S. at 411.

96. *Id.* at 414, 414 n.5.

97. *Id.* at 414 n.5, 416 (2013).

probable. Without knowing the motives or subsequent actions of unauthorized parties that cause data breaches or acquire the compromised data, these victims face a very substantial obstacle in attempting to satisfy the "actual or imminent" requirement.

B. CIRCUIT SPLIT ON INJURY IN FACT

While data breach cases pose substantial questions and novel problems for establishing Article III standing, the Supreme Court has yet to specifically address this issue in context. This issue of analyzing injury in fact for Article III standing in data breaches, however, has resulted in a circuit split among the U.S. courts of appeals. While courts recognize the injury in fact in cases in which plaintiffs have suffered from actual harm and occurrences of identity theft,[98] there is substantial disagreement over their willingness to acknowledge more speculative harms and the amount of risk sufficient to satisfy the concreteness and imminence requirements. As standing was rejected in *Clapper* for being too speculative, many circuits have focused on how this decision influences the considerations and facts in data breach cases,[99] as well as the effect of the *Spokeo* analysis on the "concreteness" prong.

1. *Circuits More Favorable to Standing in Data Breach Cases*

Some courts appear more favorable to finding standing in data breach cases and have adopted expansive or liberal theories to Article III standing. These courts include the Sixth, Seventh, Ninth, and D.C. Circuits. For example, the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC* found a sufficiently substantial risk of future harm to data breach victims who had their credit cards stolen by hackers.[100] In distinguishing the "highly attenuated" and "highly speculative" chain of events in *Clapper*, the Seventh Circuit noted that the hackers deliberately targeted Neiman Marcus to obtain customer credit card information, and it was clear what information had been subsequently stolen.[101] This amounted to a

98. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012).

99. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (exemplifying the conservative theory of standing); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (exemplifying the liberal theory of standing).

100. *Remijas*, 794 F.3d at 693.

101. *Id.* (citing *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)).

very real and immediate risk — an "objectively reasonable likelihood" of injury — that the personal data would be misused by hackers.[102] The Seventh Circuit appeared to favor standing over the mere fact that the hack occurred, stating: "[W]hy else would hackers break into a store's database and steal consumers' private information?"[103] Upon addressing mitigation expenses, the Seventh Circuit in *Remijas* once again distinguished the speculative harm in *Clapper* "based on something that may not even have happened" to data breach cases in which the initial breach has already taken place.[104] Furthermore, the court noted the credit card monitoring services that the defendant offered to consumer-victims of the data breach supported a finding of quantifiable, concrete injury.[105]

While *Clapper* involved plaintiffs that suffered actual harm from fraudulent credit card charges, the Seventh Circuit nonetheless endorsed standing on the allegations of future harm.[106] Both "increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft" have been found to be "certainly impending" and sufficiently imminent.[107] The Seventh Circuit has reinforced its expansive position on standing by finding that data breach victims suffered a "substantial risk of harm" when their debit card information was stolen in a breach and "would be used" for fraudulent purposes. As this finding satisfied the "imminence" element, mitigation expenses and efforts sufficiently amounted to "concrete injuries."[108]

The Ninth Circuit has established a similar stance towards Article III standing in data breach cases, finding sufficient injury in fact for victims who spent time monitoring their accounts but had yet to experience any actual financial losses. In a case involving a stolen laptop containing unencrypted personal data, the court found that the plaintiffs faced a credible, real, and immediate threat of harm over having their data stolen but not yet misused.[109]

---

102. *Id.* (quoting *Clapper*, 568 U.S. at 410).
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966 (7th Cir. 2016) (citing *Remijas*, 794 F.3d at 691–94).
108. *Id.* at 967.
109. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); *see also In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (finding that *Krottner*, 628 F.3d 1139, remains good law after Clapper v. Amnesty International USA, 568 U.S. 398 (2013)), *cert. denied sub nom.* Zappos.com, Inc. v. Stevens, 139 S. Ct. 1373 (2019).

The Sixth Circuit has also essentially followed in the same reasoning as the Seventh and Ninth Circuits.[110]

In *Attias v. Carefirst, Inc.*, involving a data breach of a health insurance provider, the D.C. Circuit similarly found that the plaintiffs met the "actual or imminent" requirement and established sufficient injury in fact for Article III standing.[111] This court found that the past occurrence of the data breach — where "an unauthorized party has already accessed personally identifying data" — supports a plausible inference that the party has "both the intent and ability to use that data for ill."[112] Despite the present lack of any actual harm, the substantial risk of future harm to the plaintiffs exists for injury in fact, "simply by virtue of the hack and the nature of the data."[113]

2. *Circuits Less Favorable to Standing in Data Breach Cases*

In contrast to the previously mentioned courts, the Third, Fourth, and Eighth Circuits have adopted more conservative or restrictive approaches to standing in data breach cases. Unlike the Sixth, Seventh, Ninth, and D.C. Circuits, these U.S. courts of appeals have not read into the occurrence of a breach to find a substantial risk of future harm sufficient for injury in fact. The more conservative approach adopted by these courts often requires actual evidence that the data stolen in breaches was actually used in a manner detrimental to the victims.

---

110. *See* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x. 384, 388 (6th Cir. 2016) (internal citations omitted) ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints. Thus, although it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable.").

111. Attias v. Carefirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017) (citing *Remijas*, 794 F.3d at 693). In a subsequent case, the D.C. Circuit also found that the risk of future harm, with actual occurrences identify theft, supported the conferral of Article III standing. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 56 (D.C. Cir. 2019) ("[W]e conclude that not only do the incidents of identity theft that have already occurred illustrate the nefarious uses to which the stolen information may be put, but they also support the inference that [the plaintiffs] face a substantial — as opposed to a merely speculative or theoretical — risk of future identity theft.").

112. *Attias*, 865 F.3d at 628–29.

113. *Id.* at 629 ("No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.").

As one of the first U.S. courts of appeals to reject standing in a major data breach case, the Third Circuit, in *Reilly v. Ceridian Corp.*, maintained that a plaintiff lacks standing if the alleged injury "stems from an indefinite risk of future harms inflicted by unknown third parties."[114] While the Seventh Circuit is willing to speculate on the harmful motives of actors causing data breaches to favor data breach victims,[115] the Third Circuit rejected this reasoning, opting to emphasize the reliance on numerous speculations "that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [plaintiffs] by making unauthorized transactions in [plaintiff's] names."[116] Furthermore, the large-scale nature of data breaches could reduce the likelihood that the information of any individual victim is actually exploited following the breach. The lack of accompanying allegations of actual harm seemed to be dispositive in *Reilly*, as the court distinguished the case from other circuit cases finding sufficient standing by indicating the lack of evidence that the hacker's intrusion was actually "sophisticated, intentional and malicious."[117] Similar to the reasoning in *Clapper*, the Third Circuit denied finding costs incurred by the plaintiff-victims in response to speculative future harm as supporting the conferral of injury in fact, as the costs are not in response to any actual harm.[118]

A similar position has been laid out by the Eighth Circuit, which conferred standing in a data breach case because one out of the numerous plaintiffs actually suffered an actual injury of fraudulent credit card charges.[119] Upon discussing the issue of future injury of identity theft, the court cited *Clapper* to reject the theory that stolen data without actual misuse by the hacker is sufficient for injury in fact.[120] Likewise, the Fourth Circuit in *Beck v. McDonald* emphasized the lack of allegations of actual injury, which "in turn renders [plaintiffs'] contention of an enhanced risk of future

114. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 (1992)).

115. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

116. *Reilly*, 664 F.3d at 42.

117. *See id.* at 44 (citing Pisciotta v. Old National Bancorp, 499 F.3d 629, 632 (7th Cir. 2007); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010)).

118. *See Reilly*, 664 F.3d at 46.

119. *See In re* SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017).

120. *Id.* at 770–71.

identity theft too speculative."[121] In turning to the element of "substantial risk" of future harm as a means to establish injury in fact, the Fourth Circuit rejected the plaintiffs' statistics-based conclusions that proof of thirty-three percent of individuals in the data breach becoming victims of identity theft amounts to a substantially high degree of risk.[122] Moreover, the Fourth Circuit refused to allow an organization's offers of credit monitoring as proof in support of the substantial risk of future harm, stating that it would discourage goodwill.[123] Finally, citing *Clapper* once again, the circuit straightforwardly rejected the cost of mitigative measures undertaken by data breach victims as sufficient for constituting injury in fact, calling it "self-imposed harm" in response to a speculative threat.[124]

As demonstrated above, this issue of establishing injury in fact for Article III standing in data breach litigation has resulted in a circuit split.[125] Some circuits have taken a restrictive approach to conferring Article III standing in the context of data breach cases, emphasizing speculations such as whether the information was actually accessed or whether the perpetrator had the intent and ability to make use of the compromised data.[126] These circuits heavily favor a finding of harm actually suffered, interpreting *Clapper* to have significantly raised the bar for finding sufficient speculative harm or substantial risk of future harm.[127] Alternatively, other circuits have acknowledged the harmful exposure experienced by data breach victims as sufficient for injury in fact. After laying out the requirements of establishing injury in fact for Article III standing and how the elements have been interpreted, this Note continues with the most prevalent theories of harm that plaintiffs have attempted in seeking recovery in data breaches.

---

121. Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017); *see also* Hutton v. Nat'l Bd. of Examiners in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018) (reaffirming *Beck*, 848 F.3d 262, while finding injury in fact for the plaintiffs because they allege that "they have already suffered actual harm in the form of identity theft and credit card fraud").

122. *Beck*, 848 F.3d at 274.

123. *Id.*

124. *Id.*

125. For an in-depth analysis on the circuit split among the U.S. courts of appeals, as well as district courts, see generally Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79 (2017).

126. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

127. *See supra* Part III.B.2.

C. COMMON THEORIES OF HARM RAISED IN DATA BREACH LITIGATION

Plaintiffs have sought to establish injury in fact attributable to service providers based upon different characterizations of data breach harms. As mentioned above, these theories are often found in tort law and include the following: identity theft, increased risk of future harm, and emotional distress. Plaintiffs have also attempted to analogize data breach harms, albeit unsuccessfully, to toxic torts and environmental injuries, as well as with products liability cases (e.g., defective medical devices). These theories of harm will be discussed in order of success and recognition as cognizable injuries. It is also worth mentioning that these cases are typically brought as class actions due to the nature of data breaches implicating the personal information of numerous individuals. As such, these theories of harm are typically raised together, as a means of increasing the chances of success in establishing standing.

The primary and most successful harm that can be shown to establish Article III standing in data breach litigation has been the actual occurrence of identity theft suffered by a breach victim. Many of the earliest recognitions of standing for data breach recovery included plaintiffs alleging this injury.[128] These claims are typically supported by allegations that identity theft is the likely goal of the perpetrators of data breaches, as well as the primary means in which malicious actors are able to benefit from the stolen data on large numbers of individuals.[129] This can be either by hackers directly engaging in identity theft or by selling the data to other malicious actors. The actual, concrete, and particularized nature of this harm is felt by victims of identity theft as they are typically forced to pay high costs and sacrifice massive amounts of time to fully recover and clear their names or credit scores.[130] The actual occurrence of identity theft as a data breach harm has transcended the circuit split on injury in fact, as "[n]obody doubts that identity

128. *See supra* Part III.B.

129. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

130. Cody Greadler, *The Real Cost of Identity Theft*, EXPERIAN: CSID (Sept. 9, 2016), https://www.csid.com/2016/09/real-cost-identity-theft [https://perma.cc/T5NG-62ZK] ("The DOJ's study found that victims experienced a combined average loss of $1,343. In total, identity theft victims lost a whopping $15.4 billion in 2014.").

theft would constitute a concrete and particularized injury" for purposes of Article III standing.[131]

Another harm often alleged in the event of a data breach is the increased risk of future harm. As mentioned above, whether this theory of harm is sufficient for injury in fact has largely been the focus of the circuit split among the U.S. courts of appeals. This theory is tied to the *threat* of actual harm — namely, the threat of identity theft — as plaintiffs claim information compromised in data breaches will likely be used for this purpose. The underlying reasoning of this theory of harm is embodied in the Seventh Circuit's somewhat rhetorical question: "[W]hy else would hackers break into a store's database and steal consumers' private information?"[132]

Closely related to this theory is the harm suffered by plaintiffs in the form of expenditures to reduce the risk of future harm. While the Supreme Court in *Clapper* indicated that plaintiffs could not manufacture their own injuries through mitigative expenses, many plaintiffs have argued that the expenditures are reasonably incurred in response to a substantial risk of future harm in a manner that is sufficient for injury in fact.[133] The success of this theory is largely dependent on how the injury is characterized as it has found success in other tort claims, such as toxic torts.[134]

Emotional distress is often another theory of harm that is proposed in data breach cases, yet it seems to be relatively disfavored and not given as much attention by courts.[135] This may be partly attributed to the fact that the harm could be easy to manufacture and difficult to disprove. Plaintiffs, however, will likely continue to argue emotional distress as courts have been more receptive and readily accepting of it in other contexts.[136] This argument may also be more compelling with different types of information being exposed, as they implicate different magnitudes of privacy interests.

This theory of harm may be particularly successful in contexts where the emotional distress seems objectively reasonable. While

131. Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017).

132. *Remijas*, 794 F.3d at 693.

133. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013).

134. *See* SOLOVE & SCHWARTZ, *supra* note 11, at 962.

135. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 40, 42–46 (3d Cir. 2011) (specifically addressing plaintiffs' allegations of increased risk of future harm and incurred monitoring costs but containing little discussion on emotional distress).

136. *Id.* at 44 (noting that courts have allowed plaintiffs to recover for emotional distress suffered in the toxic tort context).

the objective harms of privacy intrusions in data breaches — e.g., hackers stealing credit card information to subsequently commit identity theft — are easily identified, subjective harms are focused on less-quantifiable mental effects, such as unwanted observation of one's data or personally identifiable information.[137] While harder to argue and establish in court, the subjective harms that individuals experience can be significant and substantial, often in the form of anxiety, apprehension, and vulnerability over threats, such as knowing that your identity could be stolen.[138] The failure by courts to recognize this type of harm in data breach contexts seems unusual in light of other recognized subjective tort harms, such as the apprehension of unwanted contact in the tort of assault.[139] Nonetheless, courts addressing standing in these cases have been quick to dispose of claims based on emotion and fear.[140] Scholarship, on the other hand, has recognized the potential and need for courts to give increased attention to risk and anxiety as data breach harms.[141]

With the threat of many courts rejecting the above theories as insufficiently "visceral and vested" harms,[142] plaintiffs have also analogized data breach litigation to toxic torts and environmental injuries, as well as products liability cases. These comparisons, however, have often been quickly rejected and distinguished by courts analyzing data breach cases.[143] For example, in rejecting these analogies, the Third Circuit emphasized that toxic torts,

137. *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 (2011).

138. *Id.*

139. *Id.* at 1143 ("The subjective and objective categories of privacy harm are distinct but not entirely separate. Assault and battery are two distinct torts. Each can occur without the other. They have different elements. These two torts are nevertheless linked in that one is the apprehension of the other. The harm of assault is an internal or subjective state, specifically, the apprehension of unwanted touching. The harm of battery is the unwanted physical contact itself. . . . The two components of privacy harm are related in an analogous way. Objective privacy harm is the actual adverse consequence — the theft of identity itself or the formation of a negative opinion — that flows from the loss of control over information or sensory access. Subjective privacy harm is, by and large, the perception of loss of control that results in fear or discomfort. The two categories are distinct but related. They are two sides of the same coin: loss of control over personal information.").

140. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 272 (4th Cir. 2017).

141. For a discussion on the failure of courts to appreciate the intangible, but real harms of data breaches, as well as the costs of ignoring them, see Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018).

142. *See* SOLOVE & SCHWARTZ, *supra* note 11, at 960.

143. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011).

unlike many data breach cases, involved injures that have undoubtedly occurred, such as chemical exposure damaging human cells.[144]

This is in contrast to many data breach cases in which many plaintiffs see "no change in the status quo," such as on their credit card statements.[145] In analogizing the environmental injuries or pollution, plaintiffs also unsuccessfully attempt to draw similarities over the lack of monetary compensation as an adequate remedy.[146] Courts have rejected these arguments, stating that, unlike environmental injuries that may result in the loss of priceless mountains, the loss in data breach cases is often "simple cash."[147] Some scholars have argued that the harms in data breach cases can be like a form of pollution, involving the aggregation of minor harms of many dispersed actors over a long period of time.[148] While the collective infractions create substantial harm, the dispersion may be contributing to the failure of courts to acknowledge it.[149] Alternatively, courts may be reluctant to recognize the full extent of the harm due to a multiplier problem — there would be only small gains to the individuals but huge effects of judgments on possibly small companies.[150] Nonetheless, even in circuits more favorable to finding Article III standing in data breach cases, plaintiffs proposing these types of theories have not found significant success.[151]

Some plaintiffs have also alleged financial injury and claims of unjust enrichment premised on the theory that they overpaid for products (and accompanying assurances) because the service providers failed to invest adequately in security for the acquired consumer data.[152] This theory would require an extension of the idea that the plaintiffs would not have transacted business with the service provider if they had known the lack of security precautions

144. *Id.*
145. *Id.*
146. *Id.* at 44–45 (citing Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir.2002) (holding that "monetary compensation may well not adequately return plaintiffs to their original position" because harms to the environment "are frequently difficult or impossible to remedy")).
147. *Id.* at 45–46 (3d Cir. 2011).
148. *See* SOLOVE & SCHWARTZ, *supra* note 11, at 972.
149. *Id.*
150. *Id.*
151. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 968 (7th Cir. 2016) (explicitly stating skepticism of attempted theories of harm based in product defect and property).
152. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

employed.[153] The Seventh Circuit in *Remijas* simply distinguished the cases cited by such plaintiffs, noting that they involved product liability claims against defective or dangerous products, not data breaches. The court then declined to recognize these allegations as an alternative basis for conferring standing but noted that they "[took] nothing away from the more concrete allegations."[154]

Another attempted, but ultimately unsuccessful, theory of harm is the loss of private information as an intangible commodity. This theory has been repeatedly rejected, even by the circuits taking the favorable, expansive approach to standing.[155] One reason is because it "assumes that federal law recognizes such a property right," which plaintiffs have been unable to successfully identify supporting authorities to establish.[156] Labeled as an insufficient "abstract injury,"[157] courts have often limited the theory to circumstances in which a statutory right was created.[158] Having discussed a number of existing theories proposed in data breach litigation, this Note turns to the contextual differences raised by genetic information.

IV. DATA BREACHES INVOLVING GENETIC INFORMATION RESULT IN UNIQUE AND AMPLIFIED HARMS

The differences in genetic information from other types of information compromised in traditional data breaches reveal unique and amplified harms that will be relevant for an Article III standing analysis. Part IV.A examines these differences through a few characteristics that together set genetic information apart from more traditional forms of personally identifiable information commonly aggregated and subjected to compromise in data breaches. Part IV.B then raises and discusses the potential harms that may result from genetic information data breaches, many of which are novel and extremely consequential.

---

153. *Id.*

154. *Id.* (citing *In re* Aqua Dots Products Liab. Litig., 654 F.3d 748, 751 (7th Cir. 2011)).

155. *See, e.g.*, *Lewert*, 819 F.3d at 968 (expressing skepticism that plaintiffs have a property right to their personally identifiable data to support an allegation of theft).

156. *Remijas*, 794 F.3d at 695.

157. *Id.*

158. *See, e.g.*, *Lewert*, 819 F.3d at 968 (noting that the Video Privacy Protection Act, 18 U.S.C. § 2710 (2012), created a legally protected interest in consumer PII limited to the video rental context).

A. DISTINGUISHING GENETIC INFORMATION FROM STANDARD PII

Standard categories of personally identifiable information have included both sensitive and non-sensitive information. The most common types of non-sensitive PII records found in data breaches include email addresses, passwords, usernames, and others.[159] While these more typical types of information do not inherently reveal significant insight about the individual, they can still be used by hackers to develop a better representation of the individual for purposes of identity theft.[160] On the other hand, the most sensitive PII commonly found in data breaches could be protected health and medical information or SSNs.[161] Other common types of PII compromised in data breaches have included credit and debit card information, DMV records, financial account information, names, phone numbers, travel history, passport numbers, employment information, and the like.[162]

Genetic testing, from an individual or a family member, provides numerous unique benefits from its insight into one's risk of disease, disorders, or future medical conditions.[163] Genetic information can provide predictive health and genealogical information, such as one's common traits or clues about a person's ancestry.[164] For example, disease risk and health is a major type of DTC genetic testing that allows individuals to estimate and plan for serious medical conditions, such as celiac disease, Parkinson's disease, Alzheimer's, cystic fibrosis, sickle cell disease, and many more.[165] In addition to being the focus of substantial scientific research, genetic information has been used in the field of criminal law for convictions and exonerations.[166] Despite wanting to avoid

159. IDENTITY THEFT RESOURCE CTR., *supra* note 19, at 11.
160. *Id.*
161. *Id.* at 13.
162. *Id.* at 14.
163. *See Genetic Information Discrimination*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/laws/types/genetic.cfm [https://perma.cc/C6GV-U2ZV] (last visited Mar. 26, 2020); *What Kinds of Direct-to-Consumer Genetic Tests Are Available?*, NAT'L INSTS. OF HEALTH, NAT'L LIBRARY OF MED., GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/dtcgenetictesting/dtctesttypes [https://perma.cc/22U3-6K3A] (last visited Mar. 26, 2020).
164. *See What Is Direct-to-Consumer Genetic Testing?*, *supra* note 5.
165. *What Kinds of Direct-to-Consumer Genetic Tests Are Available?*, *supra* note 163.
166. *See, e.g.*, Associated Press, *DNA Clears Accused Golden State Killer Joseph DeAngelo of 1975 Murder*, NBC NEWS (Jan. 9, 2019), https://www.nbcnews.com/news/us-news/

the chilling of genetic testing, it is important that this personal and extremely sensitive type of information receives adequate privacy protections. The propensity of genetic information to reveal so much insight into an individual justifies a close examination for establishing proper legal treatment.

The information on consumers taken in data breaches of DTC genetic testing companies could result in the traditionally proposed harms of identity theft, increased risk of future harm, and emotional distress. However, genetic information also has a unique set of characteristics that makes it different from other types of electronic information.[167] Based in "genetic exceptionalism," some scholars have argued that genetic information requires its own distinct legal jurisprudence due to its special qualities.[168] This notion is exemplified by the fact that there has been no "meaningful new privacy laws . . . in at least a decade, with one important but narrow exception relating to genetic information."[169]

---

dna-clears-accused-golden-state-killer-joseph-deangelo-1975-murder-n956566 [https://perma.cc/S4LC-RHUF].

167. *See, e.g.*, Garner & Kim, *supra* note 56, at 1241; Ajunwa, *supra* note 47, at 1257–58, 1258 n.185 ("Social scientists have taken note of the special position that genetic information occupies in society. Instead of a piece of hereditary information, genetic information has become the key to human relationships and family cohesion.") (internal citation and quotations omitted).

168. *See* Thomas H. Murray, *Genetic Exceptionalism and "Future Diaries": Is Genetic Information Different from Other Medical Information*, *in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 60, 61 (Mark A. Rothstein ed., 1997) (describing "genetic exceptionalism" as "roughly the claim that genetic information is sufficiently different from other kinds of health-related information that it deserves special protection or other exceptional measures"); James Ken M. Gatter, *Genetic Information and the Importance of Context: Implications for the Social Meaning of Genetic Information and Individual Identity*, 47 ST. LOUIS U. L.J. 423, 427–39 (2003); *see also* Ronald M. Green & A. Mathew Thomas, *DNA: Five Distinguishing Features for Policy Analysis*, 11 HARV. J.L. & TECH. 571, 572–87 (1998) (arguing that genetic information is distinguishable due to the following features: informational risks, the longevity of DNA, DNA as an identifier, familial risks, and community impacts); Samual A. Garner & Jiyeon Kim, *supra* note 56, at 1241 ("[S]everal important features of genetic information strongly support genetic exceptionalism: familial nature, predictive ability, function as a unique identifier, stability and immutability, and potential for discrimination and stigmatization based on genetic information."). Other scholars, however, have argued against the need and recommendation of special treatment for genetic information. *See* Ajunwa, *supra* note 47, at 1258 n.187 (collecting sources); Lainie Friedman Ross, *Genetic Exceptionalism vs. Paradigm Shift: Lessons from HIV*, 29 J.L. MED. & ETHICS 141, 141 (2001) (comparing HIV with genetic information and concluding that genetic information is not exceptional); Lawrence O. Gostin & James G. Hodge, Jr., *Genetic Privacy and the Law: An End to Genetic Exceptionalism*, 40 JURIMETRICS J. 21, 23–24 (1999) (arguing against genetic exceptionalism partly on the basis of how closely genetic information melds with other medical information).

169. Ohm, *supra* note 39, at 1137 n.54 (stating that GINA was the "first new substantial category of sensitive information to gain Congressional recognition in over a decade" as the next most recent federal sensitive information law was Gramm-Leach-Bliley of 1999).

1. *Sensitivity*

Another significant characteristic separating various types of PII, including genetic information, is the degree of perceived "sensitivity." There is not a consistent scholarly definition of "sensitive information" across information privacy contexts, but many uses of the term focus on the serious damage and risk of future harm resulting from the loss of control over the information.[170] Information is often deemed sensitive if it has a high probability of being used to cause harm, contains the presence of shared confidentiality, and risks of majoritarian concerns.[171] For example, the label of "sensitive" may be attached to information that, if improperly disclosed, would often lead to stronger feelings of humiliation, abasement, or ostracism.[172] These implications typically increase the value of the information to both the data subject seeking to keep the information private and any malicious actors seeking to exploit the information for personal benefit.

Information commonly labeled as "sensitive" has been increasingly subject to compromise, as there was a 126% increase in exposed consumer records containing sensitive PII in 2018.[173] The frequency at which sensitive information is being targeted seems to be a recognition of its increasing value. As such, the negative impacts of failing to properly recognize and appreciate the implications of data breaches involving sensitive information will only worsen.

The principle that consumer information of heightened sensitivity deserves heightened protections has long been recognized and has provided the basis for targeted regulations and privacy

170. *See id.* at 1133.

171. *See id.* at 1161; *see also id.* at 1169 ("Because lists of sensitive information tend to be defined by majoritarian institutions, most importantly legislatures and administrative agencies, they tend to reflect majoritarian interests. This is an underappreciated bias that takes three distinct forms. First, categories of information are likelier to be deemed sensitive when a large segment of the population can imagine being harmed by the uncontrolled revelation of the information. . . . Second, categories that do not lead to harm to a large segment of the population are nevertheless protected as sensitive if the ruling majority can relate to the affected minority. . . . Third, the mechanisms that define sensitive information do not account for idiosyncratically sensitive information, categories of information that trigger harm, but only for a very small number of people.").

172. *See id.* at 1163 (citing Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 8 (2007)).

173. IDENTITY THEFT RESOURCE CTR., *supra* note 19, at 9.

laws.[174] In particular, health information has been commonly treated as one of the most sensitive categories, receiving congressional recognition with the passage of the Health Insurance Portability and Accountability Act of 1996.[175] Moreover, nearly every state has protections in place for various types of health information.[176] While health information is broadly considered to be more sensitive than others, the extent of sensitivity can also be applied to specific subcategories, such as genetic information.

Genetics is often treated as a subcategory of health information, deserving the label of "sensitive" and heightened protections. This is in large part due to its value in measuring and predicting health conditions. However, genetic information has been given particular attention with protections under both HIPAA[177] and state legislation across the country.[178] This can be contrasted with other increasingly-used types of information such as biometrics, for which states have been slower to adopt laws for specific privacy protections.[179]

Despite being covered under statutes generally regulating health information, genetic information became the focus of additional, targeted protections in the passage of the Genetic

174. *See, e.g.*, Ohm, *supra* note 39, at 1152 ("In passing GINA, lawmakers recognized that 'discrimination based on a person's genetic identity is just as unacceptable as discrimination on the basis of race or religion.' The law was based on the notion that '[a] person's unique genetic code contains the most personal aspects of their identity,' and the law was a response to Americans' 'legitimate fears about how this deeply private information will be used.'") (citing 154 CONG. REC. S3363-01 (Apr. 24, 2008) (statement of Rep. Kennedy)).

175. *See generally* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1938 (1996) (setting out special protections for health information by Congress).

176. *See* Ohm, *supra* note 39, at 1151–52.

177. HIPAA regulations were amended in 2013 to include "genetic information" in the definition of "protected health information." *See* 45 C.F.R. § 160.103 (2013); *see also* Application of HIPAA regulations to genetic information, 42 U.S.C. § 1320d-9 (2013).

178. *See generally Genome Statute and Legislation Database*, NAT'L INSTS. OF HEALTH, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/about-genomics/policy-issues/Genome-Statute-Legislation-Database [https://perma.cc/27HW-PGY5] (last updated Jan. 10, 2020) (last visited Apr. 2, 2020) (comprising of state statutes and bills related to genomics introduced during the 2007–2020 U.S. state legislative sessions).

179. *See* Ohm, *supra* note 39, at 1143 (citing Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475 (2013)). Biometric privacy laws have only become a recent trend, as less than five states had such legislation as of March 2019. *See* Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/FT7B-C7DK].

Information Nondiscrimination Act in 2008.[180] With this legislation, Congress recognized genetic information as the "first new substantive category of sensitive information" in over a decade.[181] While the label of "sensitive" attaching to genetic information may justify increased attention to the resulting harms and consequences of its compromise, this characteristic alone does not separate it from other forms of "sensitive" information. Even if genetic information is considered more sensitive than other types of health or medical information, its additional characteristics of immutability and informational richness create the combination that truly sets it apart.

2. *Immutability*

Another significant characteristic of genetic information that distinguishes it from other PII is its immutability. Unlike usernames, passwords, credit card numbers, and other types of information largely used for identity theft, genetic information cannot be changed in the face of fraud and theft.[182] Lacking a simple, quick solution — namely, changing the relevant information — to prevent accompanying harms, PII with longer life spans is often deemed more valuable in resale to malicious actors, especially in the context of financial and credit card information.[183] Immutability extends this consideration to the absolute by lasting indefinitely.

Immutability could also provide for an ongoing, perpetual intrusion into personal genetic privacy following disclosure to unauthorized or malicious actors. This immutability can be particularly problematic when coupled with the difficulties in truly de-identifying or anonymizing genetic data.[184] Immutability alone, however, cannot justify genetic exceptionalism, because some other types of PII share this characteristic. For example, individuals cannot

---

180. *See* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008); *see also* Ohm, *supra* note 39 and accompanying text.

181. *See* Ohm, *supra* note 39, at 1137.

182. The inability to change information may support the finding of injury in fact with certain data breach harms, such as increased risk of future harm. *See, e.g.*, *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 56 (D.C. Cir. 2019) (acknowledging that while credit card numbers may be changed to prevent future misuse, certain types of information, such as birth dates and fingerprints, are "with us forever").

183. Perlroth & Metz, *supra* note 28.

184. *See* Dankar et al., *supra* note 38 and accompanying text; *see also* Gymrek et al., *supra* note 38 and accompanying text.

change their birthdays, biometrics, or historical records which may pertain to medical conditions, financials, employment, and others. As both sensitive and non-sensitive forms of information may be immutable, the significance and relevance of this characteristic centers on its potential to amplify the scope of the information's use, whether that be for beneficial or harmful purposes. Presumably, PII with longer life spans are more valuable because the scope and duration for which the information can be exploited for value is extended — to the point of indefiniteness in the case of immutable information. When considering its information richness, genetic information may be definitively distinguished from other, traditional forms of PII.

3. *Informational Richness*

The richness of information that can be acquired from an individual's personal genetic makeup is possibly the most defining difference between genetic information and other types of PII. Genetic information has a diagnostic and predictive nature that places it in a category all by itself,[185] even apart from biometrics or other health information treated with heightened sensitivity. It has the capacity to provide a high predictive value for the onset of certain medical conditions, as well as serving as a strong indicator of increased susceptibility for many others.[186] In contrast, many common types of health information implicated in data breaches only pertain to medical histories and individual conditions that have already manifested. Additionally, genetic information can also serve some of the same traditional functions of biometric information, such as being a tool for personal identification and verification. Furthermore, not only does genetic testing reveal substantial personal information on an individual, but it can also be

185. Ajunwa, *supra* note 47, at 1258 (citing United States v. Kincade, 379 F.3d 813, 842 n.3 (9th Cir. 2004) (Gould, J., concurring) ("Like DNA, a fingerprint identifies a person, but unlike DNA, a fingerprint says nothing about the person's health, propensity for particular disease, race and gender characteristics, and perhaps even propensity for certain conduct.")).

186. *See* Wylie Burke, *Genetic Tests: Clinical Validity and Clinical Utility*, 81 CURRENT PROTOCOLS HUM. GENETICS 9.15.1, 9.15.4–9.15.5 (2014); *see also* Joyce J. Shin, Comment, *Closing the Gap: Protecting Predictive Neuroscience Information from Health Insurance Discrimination*, 64 EMORY L. REV. 1433 (2015) (discussing the disparity in protections afforded to predictive genetic information and predictive neuroscience information under GINA, HIPAA, and the Affordable Care Act, and arguing that predictive neuroscience information should be protected from health insurance discrimination in the same way that genetic information is protected).

used to identify in-depth genetic characteristics of an individual's relatives.[187]

While the informational richness of genetic information has provided for extensive beneficial uses in the healthcare context, it also creates a potential for significant misuse in the form of substantial, harmful privacy invasions.[188] The vastness of its informational potential increases the magnitude of implications possible when genetic information is compromised. The fear of its misuse was a primary basis for the enactment of GINA,[189] as the first new substantial category of sensitive information to gain congressional recognition in over a decade.[190] The possible misuses of genetic information that could prove injurious to the data subjects are discussed below.

B. POTENTIAL HARMS RESULTING FROM GENETIC INFORMATION BREACHES AND THEIR EFFECT ON INJURY IN FACT

As genetic information's relatively unique set of characteristics makes it particularly valuable, its compromise is also particularly harmful. Not only will genetic information data breaches lead to amplified traditional harms, but they will also threaten substantial novel harms that are absent from the compromise of other types of PII.

1. *Genetic Identity Theft*

As the use of genetic profiles becomes increasingly prevalent as a tool for identification, genetic information has the potential to be exploited for identity theft and fraud in a manner similar to traditional forms of PII. While official uses of personal genetic profiles are yet to be prominently featured in society beyond the law enforcement context, it is easy to imagine a future in which private

187. *See, e.g.*, Rachel Becker, *Golden State Killer Suspect Was Tracked Down Through Genealogy Website GEDmatch*, VERGE (Apr. 26, 2018), https://www.theverge.com/2018/4/26/17288532/golden-state-killer-east-area-rapist-genealogy-websites-dna-genetic-investigation [https://perma.cc/Z8WX-WNMD].

188. Robbie Gonzalez, *Your Biggest Genetic Secrets Can Now be Hacked, Stolen, and Used for Target Marketing*, IO9 (Jan. 17, 2013), http://io9.com/5976845/your-biggest-genetic-secrets-can-now-be-hacked-stolen-and-used-for-target-marketing [https://perma.cc/4KGY-GGMY].

189. Genetic Information Nondiscrimination Act of 2008, H.R. 493, 110th Cong. § 2 (2008).

190. Ohm, *supra* note 39, at 1137.

or government benefits and other registration processes are tied to one's genetic profile for identification. This would provide for a similar form of identity theft that could be used to falsify registration records or steal another's monetary benefits. Genetic information identify theft could also be perpetrated by deploying concrete DNA evidence samples, which can be replicated and fabricated to impersonate others. This form of use could be particularly dangerous to situations involving law enforcement or crime scenes.[191]

In addition to encapsulating the same risks of identity theft arising from traditional forms of PII, the harms and implications flowing from genetic identify theft will be further amplified, largely due to its previously discussed characteristic of immutability.[192] The threat of malicious actors taking advantage and assuming the identities of data breach victims will be greater due to the inability of victims to fully recover control over their genetic information. Unlike traditional data breach victims that can change their credit card numbers or create new financial accounts, the immutability of genetic information prevents compromised individuals from simply changing their genetic profiles as a means to combat fraud. Furthermore, these victims may never be able to distance themselves from the information through anonymization.[193]

A possible counter to the creation of amplified harms from genetic identity theft is the high-level of sophistication that may be needed to fully exploit genetic information — common hackers may have a limited ability to understand and make use of the data.[194] While hackers are more likely to be able to use credit card numbers to commit financial identity fraud than exploit genetic information, this comparative ease could change depending on how genetic profiles are used in the future. Nevertheless, these actors have the alternative option of selling the data sets to other malicious and more capable actors, which is often the case with

191. Andrew Pollack, *DNA Evidence Can Be Fabricated, Scientists Show*, N.Y. TIMES (Aug. 17, 2009), https://www.nytimes.com/2009/08/18/science/18dna.html [https://perma.cc/A92W-EL4H].

192. *See supra* Part IV.A.2.

193. *See generally* Yaniv Erlich & Arvind Narayanan, *Routes for Breaching and Protecting Genetic Privacy*, 15 NATURE REV. GENETICS 409 (2014) (outlining a number of data breaching and data mining techniques that are used to conduct identity tracing attacks with basic demographic information and genetic information).

194. Mere speculation that the hacker "read, copied, and understood" the information and "is able to use such information" is insufficient. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

information stolen in data breaches. As lucrative sales of the data will continue to be an option, there will remain an incentive for the theft.

While instances of genetic identity theft may be dependent on the uses of genetic information for identification, the characteristics of genetic information raise the degree of implicated risk to support finding a "substantial risk of harm" over other injuries. This is discussed further in depth below.

2. *Increased Risk of Future Harm*

Compromised genetic information creates an indefinite risk of future harm, one that is substantially greater than the risk generated from the compromise of traditional forms of PII. In order to assess the full extent of this possible harm, it is important to recognize that the risk of future harm created in data breaches is not a single occurrence with a diminishing effect following the incident, but rather it is a continuing long-term risk amounting to a wrong.[195] While circuits disagree over whether and how increased risk of future harm amounts to a sufficient injury, there is a stronger argument for individuals being forced to change their behavior when their genetic information is compromised. For example, the immutability of genetic information could lead individuals to invest in monitoring services indefinitely. Even if the risk is considered minor at one point, it becomes excessive over time, especially amounting to a sizable impact across a large number of users.[196] The ways in which a single set of genetic information could be exploited is also likely to increase as scientists unlock new predictions and uses for genetic information. As mentioned above, more detailed information often proves to be more valuable in the sale to malicious actors looking to take advantage of stolen data.[197] The informational richness and potential of genetic information is undeniable, which will likely drive its value higher than many other forms of information, as well as the incentive for theft and exploitation.

Courts commonly holding that increased risks of future harm are too speculative for standing need to sufficiently recognize that the data compromise is caused by specific actions — typically with

195. Solove & Citron, *supra* note 141, at 762–63.
196. *Id.*
197. *See* Perlroth & Metz, *supra* note 28.

specific intentions — that inherently create harms. This risk is not akin to "negligence in the air," but rather a quantifiable product of commercial entities making unreasonable actions.[198] Much of this risk is the result of poor practices, attributable to inadequate cybersecurity protections of the service provider. This amounts to harm and losses that are only amplified in the context of genetic information.

Additionally, unauthorized use of genetic information is more difficult for the owners to detect due to a comparative lack of institutional safeguards in place to flag misuse. Individuals who have their genetic information actually used by malicious actors will lack the ability to immediately identify such occurrences. This can be starkly contrasted from situations concerning traditional data breach victims who can more easily identify misuse, such as of unauthorized credit card charges appearing on financial statements. This consideration may also increase the likelihood that malicious actors can successfully exploit stolen genetic information, further increasing the implications and risk of future harm.

Genetic information's sensitivity, immutability, and richness will amplify the accompanying increased risks of future harm. This harm itself, in addition to being connected to the possibility of genetic identify theft, may also be tied to the risks of other specialized harms, such as genetic discrimination and blackmail.

3. *Genetic Discrimination and Genetic Blackmail*

Genetic discrimination and genetic blackmail are two additional harms that could flow from data breaches compromising genetic information. While actual occurrences should establish sufficient harms, the risk of these acts further contributes to the overall increased risk of future harm, especially combined with other theories. The harm of genetic discrimination is a serious threat posed by insights generated from the predictive nature of genetic information. Individuals who have a predisposition to serious medical conditions, such as Parkinson's disease or Alzheimer's disease,[199] would surely be partial to how, and if, this information is disclosed. If individuals had their genetic predispositions for debilitating conditions revealed to third-parties, they could be subjected to adverse treatment in both formal and informal settings.

198. *Id.*
199. *What Kinds of Direct-to-Consumer Genetic Tests Are Available?*, *supra* note 163.

For example, employers are likely to be interested in the long-term health of their employees; in fact, some companies were once known to include genetic testing as a routine part of their pre-employment screening.[200] These harms were recognized in the passage of the Genetic Information Nondiscrimination Act (GINA), which largely targeted and ended such practices.[201] GINA also prohibited the use of genetic information to discriminate in health insurance underwriting.[202]

While GINA protects against genetic discrimination in the majority of employment[203] and health insurance contexts,[204] it has had obvious limitations. For example, GINA does not cover life, long-term care, or disability insurance and does not apply to small-scale employers.[205] The protections of GINA are also limited with regard to the context of data breaches as it is "silent on the issue of wrongful disclosure of genetic information."[206] Nonetheless, GINA supports the proposition that these are substantial harms that are worthy of legal protections.

Beyond the more blatant forms of employment or insurance discrimination, there is also the potential for less overt modes of harm, including implicit bias and subtle forms of discrimination. While proof of these actions may be harder to factually establish in court, it is easy to foresee a scenario in which an employee's actions are questioned or more heavily scrutinized following the disclosure that the individual has a substantial chance of developing a genetic

---

200. *See* Ohm, *supra* note 39, at 1152 (citing Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1269 (9th Cir. 1998) (involving an employer that included genetic tests within its pre-employment medical screening of job applicants)).

201. *See* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, Title II, § 201(a) (codified at 42 U.S.C. § 2000ff-1(a) (2012)).

202. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *"GINA": The Genetic Information Nondiscrimination Act of 2008 Information for Researchers and Health Care Professionals* 2 (Apr. 6, 2009), http://www.genome.gov/pages/policyethics/geneticdiscrimination/ginainfodoc.pdf [https://perma.cc/XZ7N-XN4F]; *see generally* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, Title II, §§ 101–106.

203. *See Genetic Information Discrimination*, *supra* note 163.

204. *Frequently Asked Questions on the Genetic Information Nondiscrimination Act*, U.S. DEP'T OF LABOR, http://www.dol.gov/ebsa/faqs/faq-GINA.html [https://perma.cc/2SLQ-FB2C] (last visited Mar. 24, 2020).

205. *See Genetic Discrimination*, NAT'L INSTS. OF HEALTH, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/about-genomics/policy-issues/Genetic-Discrimination [https://perma.cc/JF7S-V3UT] (last visited Mar. 24, 2020); *Can the Results of Direct-to-Consumer Genetic Testing Affect My Ability to Get Insurance?*, NAT'L INSTS. OF HEALTH, NAT'L LIBRARY OF MED., GENETICS HOME REFERENCE, https://ghr.nlm.nih.gov/primer/dtcgenetictesting/dtcinsurancerisk [https://perma.cc/G7EE-HNB9] (last visited Mar. 24, 2020).

206. Ajunwa, *supra* note 47, at 1239 (citing the Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881).

disorder involving cognitive impairment — e.g., Alzheimer's. If genetic profiles containing such information became widely available, individuals could face genetic discrimination in other social settings or technological contexts, such as on dating applications. While discrimination in these contexts will likely be difficult to prove, courts need to properly acknowledge the threats of these genetic information-based harms.

The same stigmatization and adverse treatment, or fears of such treatment, that can result in discrimination can provide the basis for, and give rise to, genetic blackmail. This theory of harm is premised on the idea that individuals may be partial to disclosure and protective of the predictive information that their genetic makeup may hold. As such, malicious actors who acquire the genetic information of others may be able to successfully threaten the release of such information for blackmail by preying on a victim's fear of humiliation or ostracization.

4. *Heightened Emotional Distress*

The same fears of stigmatization or desires to keep sensitive genetic information private, which may be exploited for genetic blackmail or discrimination, may also amount to the separate intrinsic harm of emotional distress. The risk and anxiety can be characterized as a fear that society will learn of one's genetic propensities and make damaging presumptions about the individual. As legislatures acknowledge the need for heightened sensitivity and protections for dealing with this type of information, greater acknowledgement of the justifying emotional harm should similarly be recognized by federal courts.

Because a genetic makeup is often viewed as the complete sum of an individual,[207] whereby people often use genetic predictions to draw inferences regarding personal traits like fitness and suitability for reproduction,[208] the fear of having genetic information released to unauthorized parties could easily cause mental suffering and anguish. As such, these are harms that courts should find more reasonable and objective. In addition to the fear of this information being released, victims may also separately feel anxiety over third-parties possessing their genetic makeup allowing them to identify personal characteristics or predictors of which the

207. *Id.* at 1261.
208. *Id.*

individual may not even be aware. While courts have been hesitant to acknowledge emotional distress in typical data breach cases, the amplified mental anguish from compromised genetic information should be interpreted as meeting the threshold to be considered a cognizable harm. It should be recognized by courts as "actual harm" for the purpose of the injury-in-fact requirement for Article III standing.

5. *Genetic Privacy Invasion*

Privacy invasions should also be recognized as actual harm resulting from the compromise of genetic information in data breaches. The need for genetic privacy is not a novel concept as privacy proponents have recognized its implications in various contexts, such as its ability to be weaponized in politics.[209] Some scholars have even argued for the need to develop specific privacy invasion torts in response to this harm.[210] Genetic privacy invasions also raise amplified harms because unauthorized disclosure is likely to result in perpetual invasions. Information that has been released can continuously impact individual privacy. Accordingly, many countries have focused on information rights based on control, as exemplified by the General Data Protection Regulation's "right to be forgotten" in the European Union.[211]

Additionally, the legal treatment of gene theft — the clandestine collection of another's genetic materials and testing without the owner's knowledge or consent[212] — exemplifies another way in which genetic privacy can be violated and result in a cognizable harm. Indeed, gene theft has been recognized as a distinct

209. *See, e.g.*, Robert C. Green & George J. Annas, *The Genetic Privacy of Presidential Candidates*, 359 New Eng. J. Med. 2192, 2192 (2008); Allie Malloy, *Trump Resumes 'Pocahontas' Moniker After Warren DNA Test*, CNN (Oct. 16, 2018), https://www.cnn.com/2018/10/16/politics/trump-warren-tweet-dna-test/index.html [https://perma.cc/4H8B-GZSL].

210. Ajunwa, *supra* note 47, at 1246 (arguing for the development of negligent disclosure of genetic information as a new privacy tort).

211. *See generally* Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right To Be Forgotten'*, 29 COMPUTER L. & SECURITY REV. 229 (2013). Some commentators have advocated for the adoption of this right in the United States specifically in the context of genetic information. *See generally* Thomas Hale-Kupiec, Note and Comment, *Immortal Invasive Initiatives? The Need for a Genetic "Right to Be Forgotten"*, 17 MINN. J.L. SCI. & TECH. 441 (2016) (arguing for the need for a right to withdraw previously authorized genetic information from research purposes).

212. *See* Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 669–70 (2011).

criminal or civil offense in multiple states.[213] While gene theft may not map directly onto the facts and harms of data breaches, particularly as liability is not being alleged against the hackers, it strengthens the proposition that unauthorized third-party takings of genetic information amount to a cognizable harm.

6. *Privacy Exposure of Third-Parties*

The need for recognizing stronger genetic privacy rights and protecting against the attendant harms is particularly consequential because of the potential for individual genetic profiles to provide insight into the genetic makeup of relatives.[214] This is a result of the predictive nature of genetic information and its ability to reveal hereditary risks and conditions, such as Huntington's disease, cystic fibrosis, hemophilia A, and hereditary breast and ovarian cancer.[215]

The value of this informational characteristic is exemplified in its use by law enforcement to further investigations into the relatives of individuals who have had their DNA tested.[216] The potential for the data gathered from genetic testing and genealogy companies to reveal information about the relatives of tested individuals received national attention in the high-profile criminal investigation and capture of the suspected "Golden State Killer" — a case in which investigators used an open-source genetic testing database to connect decades-old crime scene DNA with the genetic information of the suspect's relatives.[217]

This characteristic of genetic profiles stretches the scope of various harms from the individual who submitted to the genetic testing to third-party relatives who did not consent and were likely even less aware of the risks. In this sense, the risk and harms of

---

213. Jacob M. Appel, *'Gene-Nappers,' like Identity Thieves, New Threat of Digital Age*, NEW HAVEN REG. (Nov. 5, 2009), http://www.nhregister.com/general-news/20091105/gene-nappers-like-identity-thieves-new-threat-of-digital-age [https://perma.cc/RB44-34CV].

214. *See* Hale-Kupiec, *supra* note 211, at 468 (stating that genetic information samples "hold[ ] an incalculable reservoir of personal information about both the individual and the individual's family").

215. Agatha M. Gallo et al., *Disclosure of Genetic Information Within Families*, 109 AM. J. NURSING 65, 65 (2009).

216. *See* Heather Murphy, *Sooner or Later Your Cousin's DNA Is Going to Solve a Murder*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/us/golden-state-killer-dna.html [https://perma.cc/A9BF-MDEE].

217. Sarah Zhang, *How a Genealogy Website Led to the Alleged Golden State Killer*, ATLANTIC (Apr. 27, 2018), https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070 [https://perma.cc/E2PQ-85Y6].

compromised genetic information go beyond any other type of PII because it no longer remains simply as "personal" identifiable information. As a single individual's genetic information can provide health indicators for entire families, a relative — and a third party to the contract between the genetic testing company and the tested individual — could be exposed to the same harms previously mentioned, such as genetic identity theft, genetic discrimination and blackmail, and genetic privacy invasions.

This harm could be analogized to family members raising possible claims of intrusion upon seclusion, or increased risk of it, premised on the notion that, unlike the DTC genetic testing consumer, these relatives never made any voluntary decisions to hand over genetic data to third-parties. Admittedly, for the purposes of establishing standing and recovery for negligent disclosure against a breached genetic testing company, these third-party claims would likely be extensions of, and more attenuated than, the direct claims of the tested individuals. This consideration, however, still supports the need for further recognition of the extent and scope of harms that may flow from compromised genetic information.

Beyond claims of harm as an extension of the individual whose DNA testing data was compromised, the privacy exposure of third parties who did not agree to genetic testing could assert a separate harm centered around the controversial concept of the "right not to know" in the medical and bioethical community.[218] In the legal context, this "right" has more often arisen when a "person does not want something that others would reasonably perceive to be in an individual's best interest (or the interests of third parties)," such as a physician's civil duty to warn in the course of treating patients.[219] The harm of information exposure and privacy invasion that a third-party relative may experience over compromised genetic information may be more akin to the harms associated with the right "to be let alone," which has given rise to the torts of intrusion upon seclusion and public disclosure of private facts.[220] While the individual who subjected themselves to genetic testing had a desire to learn about their genetic makeup, relatives of these

218. *See generally* Benjamin E. Berkman, *Refuting the Right Not to Know*, 19 J. HEALTH CARE L. & POL'Y 1 (2016).

219. *Id.* at 35, 46.

220. *See* Eli A. Meltz, Note, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion upon Seclusion*, 83 FORDHAM L. REV. 3431, 3451 (2015) (citing William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960)).

individuals who may learn this information following negligent disclosure could suffer this additional harm of receiving information that was never requested or desired.

7. *Analogies to Toxic Torts, Defective Devices, and Environmental Injuries*

An alternative framework for characterizing the harms of genetic data breaches could be as injuries that justify strict liability, as in the contexts of toxic torts, defective products, and environmental injuries. It could be argued that genetic breaches are more like these torts because monetary compensation will not make plaintiffs whole; and as such, strict liability should be applied to DTC genetic testing companies.[221] This argument is centered on the immutability of genetic information, in that, once it is disclosed to unauthorized third parties, it is essentially impossible to retrieve and reestablish full control over. The differences in data breaches involving genetic information, however, will unlikely be able to bridge the gap between these torts and traditional data breach cases, limiting the likelihood that this will be a successful characterization of the harms. As courts taking restrictive approaches have been resistant to acknowledging substantial risks of harm in data breaches at all, they are unlikely to find these harms sufficient to justify strict liability.

On the contrary, the other previously-mentioned potential harms that may result from genetic information data breaches prove to be significantly different from the harms of traditional data breaches — whether they are harms unique to compromised genetic information or forms of traditional harms with amplified consequences. The occurrence of actual injury, such as identify theft or blackmail, will undisputedly continue to suffice as a basis for standing in both contexts. Genetic privacy invasions and emotional distress from genetic information compromise, however, should be acknowledged as more visceral injuries in and of themselves, not secondary harms that must accompany another "actual" injury. Likewise, increased risk of future harm, while previously rejected as a proper theory for standing by a number of federal courts, is substantially more consequential and should be treated as sufficient for standing in the genetic information context.

---

221. *See, e.g.*, Ajunwa, *supra* note 47, at 1259–60 (arguing for strict liability to be applied in tort actions involving DTC genetic testing companies).

V. CONCLUSION

As the direct-to-consumer genetic testing industry continues to proliferate with substantial portions of the United States population having their genetic profile captured, processed, and maintained indefinitely, legal doctrines must adapt to adequately protect these individuals from the potential harms resulting from genetic information compromise. In traditional data breach contexts, plaintiffs have struggled to maintain suits for recovery due to debates over whether they have experienced truly sufficient harms for standing. The answer should be much clearer in the context of genetic information.

The unique and amplified harms of compromised genetic information should favor the conferral of injury in fact when these data breach cases inevitably come before the federal courts. In this context, the circuits taking more restrictive approaches to Article III standing will be hard-pressed to maintain their justifications for rejecting standing in light of the substantial differences between genetic information and traditional personally identifiable information. Compromised genetic information results in the actual harms of genetic privacy invasions and heightened emotional distress. The risks of genetic identity theft, genetic discrimination, and genetic blackmail are also substantial and extraordinarily consequential. The sensitivity, immutability, and informational richness of genetic information not only justifies the need for additional legal protections but also presses for immediate adaptation of the relevant legal doctrines. If victims of compromised genetic information are not able to establish standing and seek legal recourse, they will be left to shoulder the full burden of these irreversible consequences.