DATA BREACHES, SELF-REALIZATION, AND NON-ECONOMIC DAMAGES: LESSONS FROM 23ANDME

Lori Andrews*
Richard Warner**

ABSTRACT: 23andMe's genetic testing service was hacked, compromising sensitive, private genetic, health, ethnic, and location information of nearly seven million people. Beyond the potential financial losses similar to those seen in data breaches of financial institutions, the loss of control of this private information compromised the individual's right to self-realization—the process by which people interact with the world around them by choosing when and how to reveal sensitive information about themselves. In a legal system reluctant to award damages for non-economic losses, we argue that loss of control of private information itself should be compensable. We analyze the psychological, social, physical, and other risks inherent in loss of control of private information and advance a legal theory for its protection.

Contents

INTRODUCTION

In 2023, hackers accessed the online records of 6.9 million users of the direct-to-consumer genetic testing company 23andMe.[1] It was one of many breaches.[2] Data breaches averaged nine a day in 2023.[3] The 23andMe breach is noteworthy nonetheless for the sensitivity of its data, which included information about users' genetic makeup, ethnicity, health, and location.[4] Some users incurred financial losses or faced the imminent risk of such losses.[5] Those who did not still suffered a loss of informational privacy, a loss of the ability to control what others did with their information.[6]

Should loss of control over private information itself be considered an actionable harm? The question is not confined to 23andMe. Breaches of sensitive information are all too common.[7] As a recent report on healthcare breaches notes,

---

* Distinguished Professor Emerita and Director of the Institute for Science, Law and Technology, Chicago-Kent College of Law, Illinois Institute of Technology. The authors wish to thank their incredible research assistant, Millicent Kochman-Sabbatino, for her work on this Article.
** Professor and Director of the Center for Law and Computers, Chicago-Kent College of Law.

[1] Lorenzo Franceschi-Bicchierai, *23andMe Confirms Hackers Stole Ancestry Data on 6.9 Million Users*, TECHCRUNCH (Dec. 4, 2023, at 9:56 PT), https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/ [https://perma.cc/DZ3S-23VB].

[2] *See Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High*, IDENTITY THEFT RES. CTR. (Jan. 25, 2024), https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ [https://perma.cc/239F-RHA2].

[3] *Id.* This estimate is a very conservative one. The Identity Theft Resource Center (ITRC) uses a narrow definition of a breach: a data breach is "an incident in which an individual name plus a Social Security number, Driver's License number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure." *Data Breaches*, IDENTIFY THEFT RES. CTR., https://www.idtheftcenter.org/data-breaches-/ [https://perma.cc/G9ES-CF93] (last visited Sep. 26, 2025). They appear to report only breaches with some connection to the United States. *See id.* Other types of unauthorized access to computers and networks can "potentially put at risk" a great deal of other sorts of sensitive information "because of exposure," so data breaches would be even more common on a broader understanding of a data breach. *See id.*

[4] *See infra* Section II.B.

[5] *In re* 23andMe, Inc. Customer Data Sec. Breach Litig., No. 24-md-03098-EMC, 2024 WL 4982986, at *1, *4 (N.D. Cal. Dec. 4, 2024).

[6] *In re* 23andMe, Inc., 2024 WL 4982986, at *4.

[7] *See* Steve Alder, *Healthcare Data Breach Statistics*, HIPAA J. (Aug. 27, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/ [https://perma.cc/C2V7-CGP5].

> 2021 was a bad year for data breaches with 45.9 million records breached, and 2022 was worse with 51.9 million records breached, but 2023 smashed all previous records with an astonishing 168 million records exposed, stolen, or otherwise impermissibly disclosed. The huge total for 2023 includes 26 data breaches of more than 1 million records and four breaches of more than 8 million records.[8]

We first argue that where unauthorized access leads to a loss of control over private information, that loss *on its own* should be legally remediable. We argue that control of private information is necessary for self-realization.[9] We then consider the extent to which this conclusion is in keeping with legal precedents and what remedy should be granted for unauthorized breach of private information.

I. BACKGROUND

23andMe launched with great fanfare.[10] In 2008, its direct-to-consumer DNA testing was named *Time* magazine's "Invention of the Year."[11] A month earlier, its CEO, Anne Wojcicki, who was at the time married to Google founder Sergey Brin, hosted a celebrity-studded "spit party" during New York Fashion Week, where attendees could have their DNA analyzed.[12] Harvey Weinstein and Rupert Murdoch's wife, Wendi, both investors in 23andMe, attended and were genetically tested, along with

---

[8] *Id.*

[9] The connection between privacy and self-realization is widely recognized. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 98 (2008) ("[T]heorists have proclaimed the value of privacy to be protecting intimacy, friendship, dignity, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, freedom of thought, democracy, reputation, and psychological well-being"); *see also* LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY (2013) (describing how people feel violated when they learn their private information had been exploited); *see also* ROBERT H. SLOAN & RICHARD WARNER, THE PRIVACY FIX: HOW TO PRESERVE PRIVACY IN THE ONSLAUGHT OF SURVEILLANCE (2021) (explaining that the loss of privacy can alter interpersonal relationships); *see also* NEIL RICHARDS, WHY PRIVACY MATTERS (2021) (positing that ordinary people feel disempowered because they lack the knowledge and skills to control the collection of their information); *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (arguing that people should find contemporary information systems troubling only when they function without regard for social norms and values).

[10] Anita Hamilton, *Best Inventions of 2008: The Retail DNA Test*, TIME (Oct. 29, 2008), https://content.time.com/time/specials/packages/article/0,28804,1852747_1854493_1854113,00.html [https://perma.cc/3WSX-LE6P].

[11] *Id.*

[12] Allen Salkin, *When in Doubt, Spit It Out*, N.Y. TIMES (Sep. 12, 2008), https://www.nytimes.com/2008/09/14/fashion/14spit.html [https://perma.cc/FPN3-EX6N].

Ivanka Trump and Jared Kushner. [13] Warren Buffett and Jimmy Buffett later took the test to see if they were genetically related.[14] They weren't.[15] Other celebrities, including Oprah, Steven Tyler, Larry David, Snoop Dogg, Benedict Cumberbatch, and George Clooney, used DNA testing to learn more about their ethnic heritage and the extent to which their DNA indicated a possible relation to a historic figure.[16] Cumberbatch was informed that he was King Richard III's third cousin, 16 times removed.[17] Clooney was told he was related to one of Abraham Lincoln's parents. [18]

Millions of other people who are not celebrities submitted their saliva samples to 23andMe to test their genetics for hundreds of genetic predispositions to diseases (ranging from breast cancer to Alzheimer's disease) so they could take preventive steps.[19] Their genetic profile also allowed them to find genetic relatives, share medical information with them, and establish who fathered whom.[20] Along with their DNA, the customers provided 23andMe with a wide range of information—their name, their birth year, where they lived, their email address, their family tree, and, in some instances, additional medical information, photos, and their credit card information.[21]

A. The Privacy Assurances

23andMe users made the company their proxy for controlling their data by transferring that data under the expectation that 23andMe would adequately safeguard it.[22] 23andMe recognized the sensitive nature of the information it was collecting and was itself generating through genetic

---

[13] *Id.*
[14] Emmie Martin, *Warren Buffett and Jimmy Buffett Took a DNA Test to See If They're Related*, CNBC (Feb. 8, 2018, at 15:38 ET), https://www.cnbc.com/2018/02/08/warren-buffett-and-jimmy-buffett-took-a-23andme-dna-test.html [https://perma.cc/XT9Z-Z2XU].
[15] *Id.*
[16] *10 Hollywood Celebrities Who Traced Their Roots Through DNA Testing*, TOP10 (Oct. 31, 2023), https://www.top10.com/dna-testing/hollywood-celebrities-trace-ancestry [https://perma.cc/RS7E-JRRG].
[17] *Id.*
[18] *Id.*
[19] Anna Claire Vollers*, 23andMe Users' Genetic Data Is at Risk, State AGs Warn*, STATELINE (May 2, 2025, at 5:00 ET), https://stateline.org/2025/05/02/23andme-users-genetic-data-is-at-risk-state-ags-warn/ [https://perma.cc/X2UV-BKRH].
[20] *The 23andMe Personal Genome Service Experience.*, 23ANDME, https://medical.23andme.com/how-it-works/ [https://perma.cc/BD54-ZMSW] (last visited Aug. 26, 2025).
[21] 23ANDME, https://www.23andme.com/membership/ [https://perma.cc/4F65-9E6S] (last visited Sep. 11, 2025).
[22] *See Your Privacy Comes First*, 23ANDME, https://www.23andme.com/privacy/?srsltid=AfmBOopq4Y3N4l6Mb7OqeBWLDk2zs9Xn1s50ahJgT_ZfDXBUuFw4CIUV [https://perma.cc/UMB2-3JQB] (last visited Sep. 19, 2025).

testing.[23] As far back as its first year's terms of service, the company acknowledged how the information it was producing for its clients (the results of their genetic tests) could be used against its clients in ways that "could have social, legal, or economic implications."[24] From the beginning in 2008, and continuing through its current versions, 23andMe has promised "robust" security.[25] Its current privacy pledge states that "since day one, we've committed ourselves to protecting your privacy."[26] 23andMe's current privacy statement says, "At 23andMe, Privacy is in our DNA."[27] Under the question "How is My Personal Information Protected?" on its customer care page, 23andMe states: "To prevent unauthorized access or disclosure, to maintain data accuracy, and to ensure the appropriate use of information, 23andMe uses a range of physical, technical, and administrative measures to safeguard your Personal Information, in accordance with current technological and industry standards."[28]

In explaining what it does to "stay a step ahead of hackers," 23andMe says it "employs a multi-layer approach," consisting of "frequent internal assessments and simulated attacks," engaging with "a community of researchers to continually test and enhance the security of our applications, ensuring robust defenses against emerging threats," and regularly conducting "other external third-party security assessments."[29]

Despite promising privacy and acknowledging the sensitivity of the information it was protecting, 23andMe did not appear to have taken the necessary steps that were standard in the industry to minimize the possibility of data breaches.[30]

B. The Hack

As early as April 2023, a hacker entered 23andMe's system.[31] He did so using "credential stuffing"—taking usernames and passwords from other

---

[23] *Id.*

[24] *Consent and Legal Agreement*, 23ANDME, https://web.archive.org/web/20081113224511/https://www.23andme.com/about/consent/ [https://perma.cc/82CT-8QGH] (last visited Sep. 19, 2025).

[25] *Id.*

[26] *Your Privacy Comes First*, *supra* note 22.

[27] *Privacy Statement*, 23ANDME (July 11, 2025), https://www.23andme.com/legal/privacy/full-version/ [https://perma.cc/5ZYT-SEWF].

[28] *How Is My Personal Information Protected?*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202907840-How-Is-My-Personal-Information-Protected? [https://perma.cc/E74X-NG4D] (last visited Sep. 19, 2025).

[29] *Your Privacy Comes First*, *supra* note 22 (click "What do you do to stay a step ahead of hackers?" to expand the section).

[30] *See infra* Section I.C.

[31] *Backgrounder: Summary of joint investigation into data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner*, OFF. PRIV. COMM'R CAN. (June 17,

data breaches and using "bots" to try those usernames and passwords on new websites rapidly.[32] Credential stuffing exploits consumers' habit of often using the same login credentials for different websites.[33]

Initially, 14,000 23andMe user profiles were breached, equating to approximately 0.1% of all 23andMe accounts.[34] From those 14,000 accounts, hackers obtained an additional 6.9 million users' information,[35] using two account functions: the DNA Relatives feature[36] and the Family Tree feature.[37] After these additional accounts were implicated, the breach is estimated to have impacted almost half of 23andMe's 14 million customers.[38]

On October 17, 2023, a hacker calling themselves Golem[39] posted about a conversation he had with Kristen, "the CEO's right-hand,"[40] probably

---

2025), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2025/bg_23andme_250617/ [https://perma.cc/KDT7-LA4J].

[32] Lily Hay Newman, *Hacker Lexicon: What Is Credential Stuffing?*, WIRED (Feb. 17, 2019, at 07:00 ET), https://www.wired.com/story/what-is-credential-stuffing/ [https://perma.cc/UGV6-SWZB]. There have been so many "mega[-]breaches" over the last few years that hackers seemingly have a large amount of credentials to work with. *Id.* In 2019, hackers created a massive aggregate credential collection totaling 2.2 billion unique usernames and passwords known as "Collection #1-5" and made it available to download for free. *Id.* Some examples of recent victims of corporate mega-breaches include Roku, LinkedIn, MyFitnessPal, Samsung, and Walmart, to name a few. *Id.*; Aaron Drapkin, *Companies That Have Experienced Data Breaches (2022-2025)*, TECH.CO (Sep. 22, 2025), https://tech.co/news/data-breaches-updated-list [https://perma.cc/V25C-PEXQ]. Ultimately, any number of the recent data breaches could have contributed to 23andMe's breach, and any credentials taken from 23andMe's breach can now be used in a subsequent attack.

[33] Newman, *supra* note 32.

[34] Rebecca Carballo, *Data Breach at 23andMe Affects 6.9 Million Profiles, Company Says*, N.Y. TIMES (Dec. 4, 2023), https://www.nytimes.com/2023/12/04/us/23andme-hack-data.html [https://perma.cc/ZJ49-9BJQ].

[35] *Id.*

[36] DNA Relatives is a service where users opt in to provide certain information to other users on the site who might be a close DNA match, including predicted relationship, ancestor birth locations and family names, and the percentage of shared DNA. *DNA Relatives: The Genetic Relative Basics*, 23ANDME, https://int.customercare.23andme.com/hc/en-us/articles/217554778-DNA-Relatives-The-Genetic-Relative-Basics [https://perma.cc/94Q5-BVTA] (last visited Sep. 19, 2025).

[37] The Family Tree feature is a visual genealogical tree consisting of a user's closest family members (up to third cousin), who have opted into the service. *The 23andMe Family Tree Feature*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/360036068393-The-23andMe-Family-Tree-Feature [https://perma.cc/5KPL-8HDY] (last visited Sep. 19, 2025).

[38] Franceschi-Bicchierai, *supra* note 1.

[39] While the gender of the 23andMe hacker going by "Golem" remains unknown, we use male pronouns throughout the article because the character of Golem of Jewish folklore, who was sometimes referred to as the enemy of Jews, was mostly depicted as male. *See* Marilyn Cooper, *Jewish Word | Golem*, MOMENT MAG (July 17, 2017), https://momentmag.com/jewish-word-golem/#:~:text=Golems%20were%20mostly%20male%2C%20though,golem%20is%20not%20a%20sin [https://perma.cc/HS7R-ZGML].

[40] anthonyd3ca, REDDIT (r/23andME), *A Message the 23andME Hacker Posted Last Night* (2023), https://www.reddit.com/r/23andme/comments/17ch7s7/a_message_the_23andme_hacker_posted_last_night/ [https://perma.cc/9R62-U56V] (sharing screenshot of post by u/Golem, REDDIT, *23andMe - Great Britain-Originated 4M Genetic Dataset* (Oct. 17, 2023, at 20:12 ET), [https://perma.cc/NZ4Y-AQ7P]).

referring to Kristen Quint of 23andMe,[41] ten days prior, where he offered to disclose the vulnerabilities in 23andMe's website and delete his copy of hacked data for $100,000.[42] He pointed out that his advice was worth that, particularly when the company's CEO had a $30,000,000 salary.[43] After Golem was allegedly led on for five days, 23andMe reported him to the FBI without making a deal.[44] After 23andMe denied a deal, Golem began to "bring this circus down on their heads" by releasing the information referenced above.[45] Golem did give 23andMe users the chance to avoid having their own information released by giving them three days to delete their accounts before he released the information.[46]

When 23andMe did not meet the demands, Golem posted information from the breach on BreachForums, a site for online criminals.[47] The October 1, 2023, post contained a link to personal data, including genomic ancestry data, full names, birth year, and regional location of one million 23andMe users.[48] In the same post, Golem said that an additional one million accounts could be made available "depending on the interest"[49] and that "raw data"[50] was subject to a fee of $5 per unit.[51] In a subsequent post on October 17, Golem released information about "wealthy families serving Zionism" following the aftermath of the hospital explosion in Gaza City that day.[52] The link from the October 17 post was set to delete after 10 downloads

---

[41] Elle Hardy, *I'm the Assistant to the CEO of 23andMe. I Do Yoga During Meetings and Answer 400 Messages a Day — Here's What It's Like*, BUS. INSIDER (Mar. 16, 2023, at 9:00 ET), https://www.businessinsider.com/day-in-the-life-executive-assistant-ceo-23andme-anne-wojcicki-2023-3 [https://perma.cc/W9U6-GQQ9].
[42] anthonyd3ca*, supra* note 40.
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] AJ Vicens, *BreachForums Replacement Emerges as Robust Forum for Criminal Hackers to Trade Their Spoils*, CYBERSCOOP (July 7, 2023), https://cyberscoop.com/breachforums-return-criminal-hackers/ [https://perma.cc/8TH9-D9ZU].
[48] *23andMe Suffers Data Breach*, DARKOWL (Oct. 20, 2023), https://www.darkowl.com/blog-content/23andme-suffers-data-breach/ [https://perma.cc/2JSV-Z5BX]. *See also* Rebecca Carballo, Emily Schmall & Remy Tumin, *23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says*, N.Y. TIMES (Jan. 26, 2024), https://www.nytimes.com/2024/01/26/business/23andme-hack-data.html [https://perma.cc/UWT6-28QE] (detailing a lawsuit alleging that people of Chinese and Ashkenazi Jewish heritage were targeted and that their genetic information had been compiled into a list following the data breach).
[49] *23andMe Suffers Data Breach*, *supra* note 48.
[50] 23andMe defines raw data as genotype "in its raw, uninterpreted format (your A's, T's, G's, and C's)," *Navigating Your Raw Data*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/115004310067-Navigating-Your-Raw-Data [https://perma.cc/AT2Z-Q4W9] (last visited Sep. 19, 2025), where a user can search for specific genes, markers, or positions of interest including the build assembly, genome coordinate, and individual combination of variants, all distinguishable for each chromosome. *See id.* (referring to the image featured in the article).
[51] *23andMe Suffers Data Breach*, *supra* note 48.
[52] Carballo, Schmall & Tumin, *supra* note 48.

automatically, but more detailed information could potentially be disclosed to anyone who "private message[d]" Golem.[53] Subsequent posts threatened to release information about Chinese users and continued to taunt 23andMe for the ease with which the hack was able to occur.[54]

In response to the hack, 23andMe users filed over 40 legal cases against the company.[55] The cases were consolidated as *In re 23andMe, Inc., Customer Data Security Breach Litigation* on April 16, 2024.[56] A settlement was agreed upon, but implementation of the settlement was delayed due to the bankruptcy of the company.[57]

C. The Security Failures

There were at least two security failures.[58] First, 23andMe did not mandate multi-factor authentication during login until after the breach.[59] Multi-factor authentication (MFA) is authentication using more than one form of identification, such as both a password and a code sent to a user's phone.[60] MFA is a standard practice for protecting sensitive data.[61] MFA

---

[53] *23andMe Suffers Data Breach*, *supra* note 48.

[54] The hacker asked 23andMe, ". . . why haven't you taken measures against [credential stuffing] even in 2023? There's only one login service on web and mobile platforms; why didn't you use captcha, turnstile, etc. . . . there's no need for email verification even for a user to download raw data . . . How did you not notice that 100,000 of your customers' accounts had been accessed? Why didn't you define a rate limit rule based on endpoint or parameter?" *Id.*

[55] *In re* 23andMe, Inc. Customer Data Sec. Breach Litig., No. 24-md-03098-EMC, 2024 WL 4982986, at *1, *2 (N.D. Cal. Dec. 4, 2024).

[56] *Id.* at *3.

[57] *See* Defense's Notice of Suggestion of Pendency of Bankr. & Automatic Stay of Procs. at 1, *In re* 23andMe, Inc., 2024 WL 498296; *What You Need to Know About 23andMe Bankruptcy and Privacy Protections*, LEGAL EXAM'R (Apr. 8, 2025), https://www.legalexaminer.com/home-family/what-you-need-to-know-about-the-23andme-bankruptcy-and-privacy-protections-for-customers/ [https://perma.cc/2N53-UCTM] ("Any ongoing litigation is automatically stayed due to the bankruptcy filing. Known impacted parties will be updated as the process moves forward."). The stay of proceedings under Chapter 11 bankruptcy takes effect automatically pursuant to 11 U.S.C. § 362(a)-(c).

[58] Complaint at 72, *In re* 23andMe, Inc., 2024 WL 4982986.

[59] *See Addressing Data Security Concerns – Action Plan*, 23ANDME: BLOG (Dec. 5, 2023, at 14:45 PT), https://blog.23andme.com/articles/addressing-data-security-concerns [https://perma.cc/9SKD-QXFD].

[60] *What Constitutes Multi-Factor Authentication? MFA Explained*, THREATSCAPE, https://www.threatscape.com/cyber-security-blog/what-constitutes-multi-factor-authentication-mfa-explained/ [https://perma.cc/HN59-GE2K] (last visited Sep. 19, 2025); *Multi-Factor Authentication*, NIST (June 12, 2025), https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication [https://perma.cc/3SUB-3YCY].

[61] *See, e.g.*, *What Constitutes Multi-Factor Authentication? MFA Explained*, *supra* note 60. "Advancements in threat actors' sophistication, along with our reliance on the internet for secure transactions and communication, has impacted the way both businesses and the general public gain access to sensitive digital environments, making MFA standard practice." *Id.*; *see also Multi-Factor Authentication*, *supra* note 60.

would have prevented or, at the very least, significantly hindered the hacker's credential stuffing.[62]

Second, the company also failed to monitor data flows in its network adequately.[63] As the hacker noted to 23andMe, "How did you not notice 100,000 of your customers' accounts had been accessed? Why didn't you define a rate limit rule based on endpoint or parameter?"[64] The hacker had to collect the data, store it on the network and then exfiltrate it to his servers.[65] It is a standard practice to monitor for such activity.[66]

II. HOW WERE THE 23ANDME USERS HARMED?

We highlight the nature of the harms to 23andMe users by contrasting them with harms that flow from a data breach that does not involve sensitive genetic, health, ethnic, and location information. Consider, for example, the data breach of a payroll processing company, Ceridian Corporation.[67] The hacker accessed financial information and the social security numbers of Ceridian's customers' employees.[68] The Third Circuit held that a breach alone was not actionable unless the hacker actually engaged in identity theft in a way that caused financial harm to the person.[69]

However, the policy reasons to provide damages to individuals when their genetic, medical, ethnic, and location information are released are greater than in the typical, financially-related data breach. In a financial information breach, the consumer faces the issue of someone using their identity in an economically harmful way, such as by charging on their credit

---

[62] *See What Is Credential Stuffing? Examples and Prevention*, SENTINELONE (July 22, 2025), https://www.sentinelone.com/cybersecurity-101/cybersecurity/credential-stuffing/ [https://perma.cc/J2DL-BQHF].

[63] *See 23andMe Suffers Data Breach*, *supra* note 48.

[64] *23andMe Suffers Data Breach*, *supra* note 48 (featuring the exact message reproduced from the post on BreachForums).

[65] Ryan Holthouse, Serena Owens & Suman Bhunia, *The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies*, ARXIV (Feb. 6, 2025), https://arxiv.org/pdf/2502.04303 [https://perma.cc/2BNY-RWLC].

[66] Cameron Hashemi-Pour & Ben Lutkevich, *What Is an Intrusion Detection System (IDS)?*, TECHTARGET (July 15, 2024), https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system [https://perma.cc/ZF8W-5T7C] (noting that it "has become a necessity for most organizations to have either an IDS or an IPS -- usually both -- as part of their security information and event management security information and event management framework"); *see generally* MICHAEL SIKORSKI & ANDREW HONIG, PRACTICAL MALWARE ANALYSIS: THE HANDS-ON GUIDE TO DISSECTING MALICIOUS SOFTWARE Part II (2012) (offering a detailed analysis of methods for tackling malware challenges).

[67] Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

[68] *Id.* at 40.

[69] *See id.* at 43. "[A] number of courts have had occasion to decide whether the 'risk of future harm' posed by data security breaches confers standing on persons whose information *may* have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative. We agree with the holdings in those cases." *Id.* (citations omitted).

card or attempting to obtain credit.[70] As the court pointed out in *Remijas v. Neiman Marcus Group*, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[71] Annoying as it is to have to obtain a new credit card or monitor your credit rating, the out-of-pocket expenses associated with such a data breach are generally quite small.[72] Only 2.6% of hacks result in the hacked information being used in an identity theft.[73] Depending on one's credit card company, there is a $50 or even a $0 limit on liability for improper purchases.[74]

The release of other types of private information can have far more dramatic consequences for a person.[75] For example, disclosing a person's genetic information can lead to discrimination, such as being turned down for a mortgage due to a predisposition to disease or losing an inheritance when one's paternity is called into question.[76] Revealing ethnic information along with an individual's name and location can lead to the physical risks of being harassed and targeted.[77] Release of other types of private information can diminish choices that an individual can make in pursuit of self-realization.[78] Consequently, we argue that the unauthorized access to genetic, health, ethnic, and location information should in itself be treated as a compensable per se harm, and we suggest extending this approach to unauthorized access to private information more generally.

A. Economic Harms

The 23andMe users whose data was breached indicate that it cost them money and time to respond to the notice of breach (including measures to prevent identity theft).[79] Some allege specific, concrete attempts at identity theft:[80] these include an inquiry on the user's credit that she had not requested

---

[70] *Id.*
[71] 794 F.3d 688, 693 (7th Cir. 2015).
[72] James T. Graves, Alessandro Acquisti & Nicolas Christin, *Should Credit Card Issuers Reissue Cards in Response to a Data Breach?: Uncertainty and Transparency in Metrics for Data Security Policymaking*, 18 ACM TRANSACTIONS ON INTERNET TECH. 1, 12 (2018).
[73] *Id.*
[74] *Id.*
[75] Carballo, Schmall & Tumin, *supra* note 48.
[76] Kaitlyn Dowling, *Genetic Discrimination in Housing and Lending: What's the Risk?*, PETRIE-FLOM CTR. (Nov. 15, 2019), https://petrieflom.law.harvard.edu/2019/11/15/genetic-discrimination-in-housing-and-lending-whats-the-risk/ [https://perma.cc/8VU6-G9XL].
[77] Carballo, Schmall & Tumin, *supra* note 48.
[78] *See* SOLOVE, *supra* note 9, at 98.
[79] Complaint at 33, *In re* 23andMe, Inc. Customer Data Sec. Breach Litig., No. 24-md-03098-EMC, 2024 WL 4982986 (N.D. Cal. Dec. 4, 2024).
[80] *Id.* at 12, 15.

(causing her to have to put a freeze on her account),[81] a compromised bank account,[82] an attempt to rent an apartment in another country with the user's identity,[83] multiple Google alerts that passwords had been compromised,[84] attempted fraudulent activity on an account,[85] multiple requests for unauthorized authentication to email accounts,[86] being contacted by a stranger through the 23andMe website inquiring about relationships to others on the site,[87] unauthorized attempts to log into the email accounts used for 23andMe,[88] having to shut down an email address and use a different one,[89] and attempts to open unauthorized accounts using private information.[90]

B. Non-Economic Harms

23andMe users also faced non-economic harms stemming from the loss of control over their information.[91] As 23andMe itself recognized in its first terms of service, disclosure of the information it was holding about users could lead to social or legal consequences for the user.[92] Users' loss of control over their private information could have psychological or social impacts, interfering with self-realization, or even physical or economic harms that do not immediately manifest (such as physical attacks due to ethnic status or loss of an inheritance due to a revelation about paternity).[93] For all users, the psychological consequences of this loss of control exist,[94] but in some cases, the physical or financial damages will not, presenting a challenge to courts determining damages under a system emphasizing out-of-pocket losses.[95]

1. Harms from Disclosure of Genetic and Other Health Information

The genetic testing available through 23andMe, the results of which were part of the data breach, included certain health predispositions to conditions like anxiety, carrier status for over 45 potential afflictions,

---

[81] *Id.* at 12.
[82] *Id.* at 15.
[83] *Id.* at 12.
[84] *Id.* at 17.
[85] *Id.* at 30.
[86] *Id.* at 40.
[87] *Id.* at 53.
[88] *Id.* at 55.
[89] *Id.*
[90] *Id.* at 62.
[91] *Id.* at 63.
[92] *Consent and Legal Agreement, supra* note 24.
[93] *Id.*
[94] *See, e.g.*, Complaint at 78, *In re* 23andMe, Inc., Customer Data Sec. Breach Litig., No. 24-md-03098.
[95] *See* Reilly v. Ceridian Corp. 664 F.3d 43 (3d Cir. 2011).

including cystic fibrosis and anemia, various traits such as likelihood of back hair, and even "wellness" items such as predicted caffeine consumption.[96] Some plaintiffs raised concerns about their breached healthcare information being used for healthcare fraud or in ways that harm them.[97] Plaintiff Eden raised special concerns about her health care information.[98] She "is very concerned about how the theft of her highly sensitive Private Information may impact her, including with respect to . . . personal healthcare information. . . ."[99]

> Plaintiff Eden has also suffered fear, anxiety, and emotional distress as a result of the release of her Private Information, including anxiety, concern, and unease about unauthorized parties viewing, sharing, and misusing her Private Information, as well as on account of knowing that her highly sensitive Private Information is no longer confidential and can be used for blackmail, harassment, intimidation, vandalism, assault, extortion, hate crimes, identity theft or fraud, and any number of additional harms against her for the rest of her life.[100]

2. Harms from Disclosure of Ethnicity

The hackers in this breach specifically targeted ethnic groups that were already at risk of harassment and attack—Jewish individuals and Chinese individuals.[101] Some 23andMe users whose data was breached expressed particular concerns because of their revealed ethnicity.[102] One plaintiff alleged she is "of a targeted ethnicity and is concerned she may be targeted by bad actors because her genetic data revealed her ethnicity."[103] Another received harassing phone calls in Mandarin Chinese from strangers who must have learned through the breach that the user was Chinese.[104]

---

[96] Vollers, *supra* note 19; *Carrier Status*, 23ANDME, https://medical.23andme.com/reports/carrier-status/ [https://perma.cc/SK37-TNBX] (last visited Sep. 22, 2025); *Wellness Reports*, 23ANDME, https://medical.23andme.com/reports/wellness/ [https://perma.cc/K52Z-HEVL] (last visited Sep. 22, 2025).
[97] Complaint at 9, 12, *In re* 23andMe, Inc., Customer Data Sec. Breach Litig., No. 24-md-03098.
[98] *Id.* at 15.
[99] *Id.*
[100] *Id.*
[101] Carballo, Schmall & Tumin, *supra* note 48.
[102] Complaint at 15, *In re* 23andMe, Inc., Customer Data Sec. Breach Litig., No. 24-md-03098.
[103] *Id.* at 64.
[104] *Id.* at 13.

Concerns about the leak of one's ethnic information are reasonable, given the overall harassment of Jewish and Chinese individuals.[105] Jewish individuals have a history of being targeted, including during the mass genocide of World War II.[106] The Anti-Defamation League (ADL) tracks antisemitic acts in the United States and publishes an annual Audit of Antisemitic Incidents.[107] The ADL reported 8,873 antisemitic incidents across the U.S. in 2023,[108] a 140% increase from 3,697 incidents recorded in 2022.[109] This is higher than the three years prior, combined.[110] Specifically, between October 7 and the end of 2023, the ADL counted 5,204 antisemitic incidents,[111] which is more than all of 2022.[112] Harassment occurred most frequently, with the ADL citing 6,535 incidents.[113] Vandalism was the second most common, with 2,177 incidents.[114] There were 161 incidents of assault.[115] Even though the ADL was recording notable increases in monthly antisemitic incidents prior to October 7, 2023, these incidents "skyrocketed to a level unprecedented in the history of ADL's tracking of antisemitism" afterwards.[116]

---

[105] *Antisemitism Explained,* U.S. HOLOCAUST MEMORIAL MUSEUM, https://www.ushmm.org/antisemitism/what-is-antisemitism/explained [https://perma.cc/Y7AY-VGMC] (last visited Sep. 17, 2025); U.S. COMM'N ON C.R., THE FEDERAL RESPONSE TO ANTI-ASIAN RACISM IN THE UNITED STATES 1 (2023), https://www.usccr.gov/files/2023-09/fy-2023-se-report_0.pdf [https://perma.cc/TMR4-TSWP].

[106] *Antisemitism Explained*, *supra* note 105.

[107] *U.S. Antisemitic Incidents Soared 140 percent in 2023 – Breaking all Previous Records*, ANTI-DEFAMATION LEAGUE (Apr. 16, 2024) [hereinafter *Antisemitic Incidents in 2023*], https://www.adl.org/resources/press-release/us-antisemitic-incidents-soared-140-percent-2023-breaking-all-previous [https://perma.cc/C6AB-CS3B].

[108] *Id.*

[109] *Audit of Antisemitic Incidents 2022*, ANTI-DEFAMATION LEAGUE (Mar. 23, 2023), https://www.adl.org/resources/report/audit-antisemitic-incidents-2022 [https://perma.cc/4DFE-V8CA].

[110] *Antisemitic Incidents in 2023*, *supra* note 107.

[111] *Id.*

[112] *Audit of Antisemitic Incidents 2022*, *supra* note 109.

[113] *Antisemitic Incidents in 2023*, *supra* note 107.

[114] *Id.*

[115] In these reports, assault is defined as cases where Jewish people (or people perceived to be Jewish) were targeted with physical violence accompanied by evidence of antisemitic animus. *Id.*

[116] *Audit of Antisemitic Incidents 2023*, ANTI-DEFAMATION LEAGUE (Apr. 16, 2024), https://www.adl.org/resources/report/audit-antisemitic-incidents-2023 [https://perma.cc/G256-Y5J4]. The ADL lists many specific incidents in their annual audit, including both physical and verbal bias-motivated actions against Jewish individuals. In California in October 2023, an individual with a knife broke into a Jewish family's home and said, "I'm going to kill you because you are Jewish," before physically assaulting one of the family members. Marc Sternfield & Myja Gary, *Studio City Home Intruder Shouted Antisemitic Insults, Victim Says*, K.T.L.A. (Oct. 27, 2023, at 20:33 PT), https://ktla.com/news/local-news/studio-city-family-targeted-in-home-invasion-suspect-shouts-free-palestine/ [https://perma.cc/Z7LT-XUUC]. That same month, an individual allegedly stated, "You think you're so tough waving a flag, Zionist shitbag, let's see how tough you are when I'm out here!" to a Jewish UMass student, before punching the student, taking their Israeli flag, and spitting on it. ANTI-DEFAMATION LEAGUE, CAMPUS REPORT DATA , 5 (2024) [https://perma.cc/GB37-XYBR]. In November of 2023, at Ohio State University, two Jewish students were punched by assailants who asked if they were Jewish and made antisemitic comments. Meredith Deliso, *Ohio State Reports 2 Antisemitic Incidents*

Attacks have also occurred against Asian Americans. In 2023, the U.S. Commission on Civil Rights wrote a report addressing Asian-American hate crimes since COVID and the federal government's response to combat such incidents.[117] A survey done by Pew Research Center of a representative sample of adults, including 352 Asian adults, found that about 81% of the Asian adults in the sample indicated that violence against them was increasing.[118] Examples include both verbal and physical assaults by passersby,[119] some leading to death.[120]

3. Harms from Disclosure of Location Information

When information about the location of an individual from a disfavored group is released, that person can be targeted.[121] During World War II, the release of location information about Jewish individuals led to their death.[122] In *Delete: The Virtue of Forgetting in the Digital Age,* Viktor Mayer-Schönberger describes how the Dutch government in the 1930s created a registration system to keep better track of its citizens.[123] The population registry listed each citizen's "name, birth date, address, religion, and other personal information" to facilitate government administration and welfare planning.[124] However, when the Nazis invaded the Netherlands during World War II, they seized possession of the registry and used it to go after the Dutch citizens who were Jewish or gypsy.[125] The repurposed registry was so comprehensive, notes Mayer-Schönberger, that the Nazis were able to identify and ruthlessly murder more than 70 percent of the Jewish population in the Netherlands, as opposed to 40 percent in Belgium and 25 percent in France, where the government records were not as precise.[126]

Against Students in 24 Hours, ABCNEWS (Nov. 10, 2023, at 16:31 ET), https://abcnews.go.com/US/ohio-state-antisemitic-incidents/story?id=104794723 [https://perma.cc/L7RS-3N8C].

[117] U.S. COMM'N ON C.R., *supra* note 105.

[118] Neil G. Ruiz, Khadijah Edwards & Mark Hugo Lopez, *One-third of Asian Americans fear threats, physical attacks and most say violence against them is rising*, PEW RSCH. CTR. (Apr. 21, 2021), https://www.pewresearch.org/short-reads/2021/04/21/one-third-of-asian-americans-fear-threats-physical-attacks-and-most-say-violence-against-them-is-rising/ [https://perma.cc/66XU-NZNT].

[119] U.S. COMM'N ON C.R., *supra* note 105, at 56.

[120] *Id.* at 94.

[121] *See* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 141 (2009) (citing William Seltzer & Margo Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses*, 68 SOC. RSCH. 481, 486 (2001)).

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Id.*

Location information has also been used to target other individuals from disfavored groups, not related to ethnic background.[127] Abortion doctors have been kidnapped from their homes at gunpoint,[128] shot,[129] and killed.[130] Their homes have been shot at[131] and their children threatened.[132] An Indiana doctor was forced to stop providing abortions after her daughter was the subject of a kidnapping threat.[133] The threat was identified by the FBI after the doctor performed an abortion on a 10-year-old rape victim who could not receive an abortion in her home state.[134] Abortion clinic staff have been threatened[135] and assaulted.[136] One such staff member, Allison Dreith, head of strategic partnerships of the Midwest Access Coalition, had to move four times after threatening letters arrived at each new location.[137] The letters came as an attempt to "scare [her] into inaction," and "led her to fear for her personal safety."[138] Clinics have been subjected to bombings,[139] Molotov

---

[127] *See, e.g., Violence to Abortion Providers*, FEMINIST MAJORITY FOUND., https://feminist.org/our-work/national-clinic-access-project/violent-attacks-on-abortion-providers-murders-attempted-murders-kidnapping/ [https://perma.cc/A5VD-R3H2] (last visited Sep. 20, 2025).
[128] *Id.*
[129] *Id.*
[130] *Man Who Killed Late-Term Abortion Doctor Gets Lighter Sentence,* CBS NEWS (Nov. 23, 2016, 20:06 ET), https://www.cbsnews.com/news/scott-roeder-man-who-killed-george-tiller-late-term-abortion-doctor-gets-new-lenient-sentence/ [https://perma.cc/84KM-DADJ].
[131] *Violence to Abortion Providers*, *supra* note 127.
[132] Mary Papenfuss, *Ohio Girl's Abortion Doctor Once Targeted In Vicious Kidnapping Threat: Report*, HUFFPOST (Jul. 17, 2022), https://www.huffpost.com/entry/caitlin-bernard-amy-coney-barrett-kidnapping-abortion-threat-organization_n_62d33382e4b0116f21bc80c4 [https://perma.cc/8YSL-HXMW].
[133] Timothy Bella & Kim Bellware, *Doctor in 10-Year-Old's Abortion Case Faced 2020 Kidnapping Threat Against Daughter,* WASH. POST (July 16, 2022), https://www.washingtonpost.com/politics/2022/07/16/abortion-girl-rape-doctor-bernard-kidnapping-barrett/ [https://perma.cc/7WPC-FRRZ].
[134] *Id.*
[135] NAT'L ABORTION FED'N, 2022 VIOLENCE & DISRUPTION STATISTICS 6, https://prochoice.org/wp-content/uploads/2022-VD-Report-FINAL.pdf [https://perma.cc/D6X2-5ERB] (last visited Sep. 20, 2025).
[136] *Id.* at 8.
[137] Avi Asher-Schapiro & Anastasia Moloney, *FEATURE-US Abortion Advocates Face Doxxing as Data Scavenged Online,* REUTERS (Aug. 1, 2023, at 11:30 ET), https://www.reuters.com/article/business/healthcare-pharmaceuticals/feature-us-abortion-advocates-face-doxxing-as-data-scavenged-online-idUSL8N39E8D3/ [https://perma.cc/Q59A-TD3X]. Ms. Dreith still appears to work at the Midwestern Access Clinic in the same role and can possibly be contacted there. The website provided neither a phone number, nor email.
[138] *Id.*
[139] *Violence Against Abortion Providers Continues to Rise Following Roe Reversal, New Report Finds,* NAT'L ABORTION FED'N (May 11, 2023, at 06:00 ET), https://prochoice.org/violence-against-abortion-providers-continues-to-rise-following-roe-reversal-new-report-finds/ [https://perma.cc/Y44A-ZP2L]. The article was based on the 2022 National Abortion Federation report. Instances of violence include a 1984 Christmas Day bombing of two doctors' offices and one abortion clinic in Florida. Liam Stack, *A Brief History of Deadly Attacks on Abortion Providers*, N.Y. TIMES (Nov. 29, 2015), https://www.nytimes.com/interactive/2015/11/29/us/30abortion-clinic-violence.html [https://perma.cc/7AEW-MX97].

cocktails,[140] and cyberattacks to disrupt clinic operations.[141] Targeting of abortion providers occurs across the country.[142] Between 2010 and 2019, there were 351 reported death threats/threats of harm to abortion providers; between 2020 and 2021, there were 382.[143]

Genetic information, health information, ethnic information, and location information are examples of information that people expect control over in order to define themselves, to ensure opportunities, and to avoid risks.[144] Such risks could include an employer not hiring an individual if he knows the person's genetic predisposition to disease or the risk of an internet troll attacking the individual if he knows the person's home address. However, an individual's act of defining themselves and controlling how others view them can be impeded by unauthorized access to a broader array of private information than was at issue in the 23andMe case.[145]

4. Harm to Self-Realization from Losing Control Over Other Types of Private Information

Loss of informational privacy in realms beyond those at issue in the 23andMe case can close windows of opportunity for self-realization.[146] Control over private information is essential to respect, trust, friendship, love, and personal liberty.[147] The connection between self-realization and informational privacy is a familiar theme in sociology.[148] As the sociologist Nippert-Eng emphasizes:

> At its core, managing privacy is about managing relationships between the self and others. . . . [P]rivacy . . . [is] a "boundary regulatory process by which a person (or

---

[140] *Recent Cases on Violence Against Reproductive Health Care Providers*, U.S. DEP'T OF J.: C.R. DIV. (May 30, 2023), https://web.archive.org/web/20250201201119/https://www.justice.gov/crt/recent-cases-violence-against-reproductive-health-care-providers [https://perma.cc/JCN5-6FZQ].

[141] Sam Sabin, *'Lock It Down Right Now': Abortion rights advocates prepare for a new wave of digital security threats*, POLITICO (June 17, 2022, at 18:16 ET), https://www.politico.com/news/2022/06/17/abortion-rights-advocates-digital-security-threats-00040654 [https://perma.cc/NU3W-DE92].

[142] NAT'L ABORTION FED'N, *supra* note 135, at 2.

[143] NAT'L ABORTION FED'N, 2021 VIOLENCE & DISRUPTION STATISTICS 14, https://prochoice.org/wp-content/uploads/2021_NAF_VD_Stats_Final.pdf [https://perma.cc/QSH7-45NK] (last visited Sep. 10, 2025).

[144] *See* SOLOVE, *supra* note 9, at 98.

[145] *Id.*; SLOAN & WARNER, *supra* note 9 (explaining that the loss of privacy can alter interpersonal relationships).

[146] *See* SOLOVE, *supra* note 9, at 98; SLOAN & WARNER, *supra* note 9 (explaining that the loss of privacy can alter interpersonal relationships).

[147] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).

[148] *See* CHRISTENA E. NIPPERT-ENG, ISLAND OF PRIVACY 22 (1996) (quoting IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 3 (1975)).

> group) makes himself more or less accessible and open to others." When we regulate our accessibility to others—including the accessibility of information, objects, space, time, or anything else that we deem private—we simultaneously regulate our relationships with them.[149]

We argue that adequate self-realization requires sufficient informational privacy and that the loss of informational privacy from data breaches is serious enough to justify treating that loss as a legally cognizable harm. As the philosopher John Gray notes,

> We are none of us defined by membership in a single community or form of moral life. We are . . . heirs of many distinct, sometimes conflicting, intellectual and moral traditions. . . . The complexity and contradictions of our cultural inheritance give to our identities an aspect of complexity and even of plurality which is . . . essential to them. . . . [T]he power to conceive of ourselves in different ways, to harbour dissonant projects and perspectives, to inform our thoughts and lives with divergent categories and concepts, is integral to our identity as reflective beings.[150]

Individuals construct their multifaceted identities by selecting what they will identify with from the possibilities open to them. We claim that adequate realization of a multifaceted self requires informational privacy.

People realize a multifaceted self by playing different social roles with different people. Consider Roger, who is a birdwatcher, prostate cancer survivor, 50% Cherokee, pro-life protestor, and is genetically predisposed to diabetes. When Roger meets his fellow birdwatchers, his goal is to relate to them as a birdwatcher, not as a birdwatcher/cancer survivor/half Cherokee/pro-life protestor/potential diabetic. In a world with minimal disclosure of data to third parties, Roger can exercise his "power to conceive of [himself] in different ways, to harbour dissonant projects and perspectives, to inform [his] thoughts and [life] with divergent categories and concepts"[151] without worrying that his activities will undermine each other. The less information about one that is available to third parties, the more enclaves of privacy one can create. Those enclaves are, to use the sociologist Christena

---

[149] *Id.*
[150] JOHN GRAY, POST-LIBERALISM: STUDIES IN POLITICAL THOUGHT 262–63 (photo. reprt. 1996) (1993).
[151] *Id.* at 263.

Nippert-Eng's apt expression, "territories of self,"[152] where "only those aspects of self that we and others deem appropriate are activated and supported at a given time and place."[153]

Disclosure of private information reduces our ability to create territories of self. Suppose, for example, that a data breach reveals that Roger is a cancer survivor, 50% Cherokee, pro-life advocate, and genetically disposed to diabetes. It also reveals his location at various times, from which one can infer which doctors, clinics, and religious institutions he visited. The disclosure increases a range of potential risks. The information that he is predisposed to diabetes may cause him to be turned down for a job;[154] his status as an American Indian can expose him to harassment;[155] revealing his location data may also lead to harassment if some of the locations are identified as institutions of a disfavored religion.[156] The disclosure that Roger is a birdwatcher/cancer survivor/half Cherokee/pro-life advocate/potential diabetic can alter his personal and work relationships. First, the unauthorized disclosure of data to unknown third parties involves a significant loss of control over the borders of our "territories of self"[157] that Roger has sought to create. Roger should not, without justification, be deprived of what is essential to managing his relationships with others: namely, the ability to set borders that are difficult to cross without permission. Second, the potential loss of that ability entails a potential risk of altered relationships as people see and react to Roger differently based on what they have learned about him.[158]

In general, the more private data is exposed to the potential gaze of others, the more the borders of our "territories of self"[159] become uncertain and porous. The more uncertain and porous, the less we can be sure that "only those aspects of self that we and others deem appropriate are activated and supported at a given time and place."[160] There is ample historical evidence

---

[152] CHRISTENA E. NIPPERT-ENG, HOME AND WORK: NEGOTIATING BOUNDARIES THROUGH EVERYDAY LIFE 68 (1996)
[153] *Id.*
[154] *Litigation Materials from Diabetes Discrimination Cases*, AM. DIABETES ASS'N., https://diabetes.org/advocacy/attorney-resources/litigation-materials-from-diabetes-discrimination-cases [https://perma.cc/W7Y6-VJJ6] (last visited Sep. 20, 2025).
[155] *See, e.g.*, Mary G. Findling et al., Discrimination in the United States: Experiences of Native Americans, 54 HEALTH SERV. RES. 1431, 1434 (2019); Understanding the High Rates of Violence Against Native Americans, STRONGHEARTS NATIVE HELPLINE, https://strongheartshelpline.org/about/understanding-the-high-rates-of-violence-against-native-americans [https://perma.cc/EFP3-J2TW] (last visited Sep. 20, 2025).
[156] *Antisemitic Incidents in 2023*, *supra* note 107.
[157] NIPPERT-ENG, *supra* note 152, at 68.
[158] *See* SLOAN & WARNER, *supra* note 9 (discussing in detail the impact of data disclosure on self-realization).
[159] NIPPERT-ENG, *supra* note 152, at 68.
[160] *Id.*

that sufficiently pervasive and invasive disclosure of information inhibits self-realization. The 1950 to 1990 East German Stasi illustrates the threat.[161] The "hidden, but for every citizen tangible omni-presence of the Stasi, damaged the very basic conditions for individual and societal creativity and development: Sense of one's self, Trust, Spontaneity."[162]

Not all losses of informational privacy, however, warrant an award of damages. Consider an extended family holiday dinner. Harmony requires a selective flow of information. Things you can say to Aunt Jane should not reach Uncle John's ears, and vice versa. No one would seriously suggest imposing legal liability on a rebellious adolescent who deliberately violates the harmony-ensuring strictures on information flows. However, non-family institutions that store (and sometimes even generate) private information should face liability for the damage they have done to the possibility of self-realization when they offer insufficient protection to such information.

III. WHAT ARE THE LEGAL PRECEDENTS FOR PROTECTION OF PRIVATE INFORMATION?

Privacy is a key value in American law.[163] As a 2001 court decision recognized, "the claim of a right of privacy is not 'so much one of total secrecy as it is of the right to *define* one's circle of intimacy--to choose who shall see beneath the quotidian mask.'"[164] Consequently, courts and legislatures have recognized the importance of what Nippert-Eng describes as the "boundary regulatory process"—being able to control who receives information about you.[165]

Courts already recognize causes of action for disclosures of medical information by institutions or individuals that provide health care services based on breach of contract,[166] violation of privacy,[167] negligence,

---

[161] *See* GARY BRUCE, THE FIRM: THE INSIDE STORY OF THE STASI 12 (2010).

[162] *Id.*; *see also* ORLANDO FIGES, THE WHISPERERS: PRIVATE LIFE IN STALIN'S RUSSIA (2007) (describing how the Stalin dictatorship instilled fear and mistrust among Soviet citizens); VACLAV HAVEL & JOHN KEANE, THE POWER OF THE POWERLESS: CITIZENS AGAINST THE STATE IN CENTRAL EASTERN EUROPE (Routledge 2015) (1985) (asserting that life in the post-totalitarian system is permeated with hypocrisy and lies); KAI STRITTMATTER, WE HAVE BEEN HARMONIZED: LIFE IN CHINA'S SURVEILLANCE STATE (Ruth Martin trans., HarperCollins Publishers 2020) (2018) (describing how dictatorships disconnect citizens from truth and reality); SLOAN & WARNER, *supra* note 9 (discussing in detail the impact of data disclosure on self-realization).

[163] *See, e.g.,* Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972).

[164] M.G. v. Time Warner, Inc., 89 Cal. App. 4th 623, 632 (2001).

[165] NIPPERT-ENG, *supra* note 152, at 22.

[166] *See* Horne v. Patton, 287 So. 2d 824, 831–32 (Ala. 1973); *see also* MacDonald v. Clinger, 446 N.Y.S.2d 801, 803–04 (App. Div. 4th Dept. 1982).

[167] *See Horne*, 287 So. 2d at 830–31 (recognizing a right to privacy to protect persons from unauthorized disclosure of medical records); *see also* Bazemore v. Savannah Hosp., 155 S.E. 194, 196 (Ga. 1930).

malpractice,[168] and breach of fiduciary duty.[169] Courts can also recognize a privacy cause of action based on interference with contractual relations[170] or infliction of emotional distress.[171] The jury award of damages can be quite high for unauthorized release of medical information and goes beyond the recovery of out-of-pocket losses to include compensation for anxiety and mental anguish.[172] In a 2018 Connecticut case,[173] for example, the plaintiff was awarded $853,000 for non-economic harm[174] when her physician's practice released her medical information to her ex-boyfriend, who then used it against her in a paternity case.[175] This is a prime example of compensating an individual for non-economic harms when unauthorized disclosure of information thwarts a person's self-realization.[176]

The importance of safeguarding healthcare information, in general, and genetic information, in particular, is underscored by statutory protections, ranging from the federal regulations under HIPAA[177] to state statutes that provide damages (in some cases, $150,000 or more)[178] to an

---

[168] *See MacDonald*, 446 N.Y.S.2d at 805–06 (Simons, J., concurring) (indicating that the basis for the plaintiff's cause of action was malpractice).
[169] *See Horne*, 287 So.2d at 827–30.
[170] *See* Charles J. Roedersheimer, Note, *Action for Breach of Medical Secrecy Outside the Courtroom*, 36 U. CIN. L. REV. 103, 117–19 (1967).
[171] *See* W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 12 (5th ed. 1984) (outlining the cause of action for infliction of mental distress).
[172] Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 175 A.3d 1, 1 (Conn. 2018).
[173] *Id.*
[174] Steve Alder, *$853,000 Awarded to Patient Whose PHI Was Impermissibly Disclosed to Former Boyfriend*, HIPAA J. (Dec. 21, 2018), https://www.hipaajournal.com/853000-awarded-to-patient-whose-phi-was-impermissibly-disclosed-to-former-boyfriend/ [https://perma.cc/BGF5-PLX7]:

> The lawsuit claimed that as a result of the disclosure of her medical records, Byrne suffered emotional distress, trauma, and anxiety, was harassed by exposure to civil claims in federal district court, received threats from [ex-boyfriend] Mendoza of criminal charges, and suffered financial losses relating to legal fees and medical bills.

Id. According to Byrne's attorney Bruce Elstein, she did not seek reimbursement for the financial losses and thus the entire $853,000 award was for emotional distress. Telephone Interview with Bruce Elstein (Oct. 11, 2024).
[175] The *Byrne* court opinion indicated that, as of 2018, all but four states recognized a cause of action for breach of a physician's duty of confidentiality. 175 A.3d at 16. However, in some instances, even absent that specific cause of action, the aggrieved patient can pursue a traditional invasion of privacy case. *Id.*
[176] *Id.* at 2.
[177] 45 C.F.R. § 164.510 (2013).
[178] Oregon Genetic Privacy Law section 192.541 provides the following statutory damages:

> (3) For a violation of ORS 192.535 [need informed consent to obtain genetic information] or 192.539 [prohibits unauthorized disclosure of genetic information], the court shall award the greater of actual damages or: (a) $1,000, for an inadvertent violation that does not arise out of the negligence of the defendant; (b) $5,000, for a negligent violation; (c) $100,000, for a knowing or reckless violation; (d) $150,000, for a knowing violation based on a fraudulent misrepresentation; or (e)

individual whose healthcare information is inappropriately released. Some of the genetic privacy statutes even include criminal penalties for unauthorized disclosure of genetic information.[179] Some data breach cases recognize health and genetic information as deserving special protection.[180]

In keeping with the precedents protecting genetic and health information, the proposed settlement in the 23andMe case awards extra damages to people whose genetic or health information was released, even where they have not shown out-of-pocket losses.[181] The settlement does not, however, take a similar approach to the unauthorized release of ethnic and location information.[182] We argue that unauthorized disclosure of such information similarly merits damages. There are legal precedents providing protection from discrimination and harm based on ethnic origin.[183] The Constitution's Equal Protection Clause protects people from discrimination based on their ethnic background because individuals of certain ethnic backgrounds have historically faced persecution and unequal treatment.[184] Similarly, under hate crime laws,[185] ethnic and minority groups receive special attention from law enforcement "because of the profound impact such crimes have on the victim, the group to which the victim belongs, and the community as a whole."[186] Under various federal and state laws, speech and physical abuse against people based on their ethnicity is subject to a higher penalty than speech and abuse that is not so targeted.[187] For example, Sidi Mohamed Abdallahi, accused of shooting a Jewish man walking to a synagogue in a Chicago suburb, [188] has, since his arrest, been subject to

---

> $250,000, for a knowing violation committed with intent to sell, transfer or use for commercial advantage, personal gain or malicious harm.

OR. REV. STAT. § 192.541 (2001).

[179] *See, e.g.*, *id.* § 192.543.

[180] *In re* Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130, 1143 (C.D. Cal. 2021) ("Courts have refused to dismiss invasion of privacy claims at the motion to dismiss stage where, as here, a data breach involved medical information, because the disclosure of such information is more likely to constitute an 'egregious breach of the social norms" that is 'highly offensive.'").

[181] Order Conditionally Granting Mot. for Prelim. Approval at 8, *In re* 23andMe, Inc. Customer Data Sec. Breach Litig., No. 24-md-03098-EMC, 2024 WL 4982986 (N.D. Cal. 2024).

[182] *Id.* at 5–6.

[183] *E.g.*, Brown v. Bd. of Educ., 347 U.S. 483, 495 (1954).

[184] U.S. CONST. amend. XIV, § 1.

[185] *See, e.g.*, The Matthew Shepard and James Byrd Jr., Hate Crimes Prevention Act, Pub. L. No. 111-84, Div. E., 123 Stat 2835 (2009) (codified at 18 U.S.C. § 249) (creating standardized penalties for violent hate crimes based on race, religion, national origin, gender, sexual orientation, gender identity, or disability).

[186] Stephen Russell Martin II, *Establishing the Constitutional Use of Bias-Inspired Beliefs and Expressions in Penalty Enhancement for Hate Crimes: Wisconsin v. Mitchell*, 27 CREIGHTON L. REV. 503, 508 (1994).

[187] *Id.* at 510.

[188] Sam Charles, *Hate crime, Terrorism Charges Added Against Alleged West Rogers Park Shooter*, CHI. TRIB. (Oct. 31, 2024, at 18:20 CT), https://www.chicagotribune.com/2024/10/31/hate-crime-terrorism-charges-added-against-alleged-west-rogers-park-shooter/ [https://perma.cc/D62H-MURH].

additional hate crime and terrorism charges.[189] The additional charges were added after an investigation into the suspect's phone revealed an intentional plan to target Jewish individuals.[190]

Location data itself has been recognized as being sensitive in the context of a data breach because it is "*likely to cause* substantial injury to consumers."[191] The 23andMe leak released ethnic data coupled with location information.[192] Such information could lead to (and appears to have been intended by the hacker to lead to) physical assaults against individuals.[193] While financial data breach cases generally only allow recovery of out-of-pocket losses,[194] requiring that physical attacks occur before compensation seems unreasonable.

In fact, a wide array of private information necessary for self-realization is legally protected. In general, people have a right to choose the context in which they wish to release information. A woman who learns she is pregnant might choose to tell her husband, but not tell her employer, if she is worried that, contrary to the Pregnancy Discrimination Act,[195] they will then choose not to promote her. Choosing which people or groups learn private information is consistent with the First Amendment's protection of freedom of association.[196] In *NAACP v. Alabama*, for example, people were entitled to keep information about one aspect of their lives (membership in the NAACP) private from other segments of society (for example, the government).[197]

Cases involving unauthorized disclosure of personal information are like defamation cases, where the disclosure itself is viewed as a per se harm.[198] In fact, in some instances, the per se harm in the defamation cases

---

[189] *See* 720 ILL. COMP. STAT. 5/12-7.1 (2022); 720 ILL. COMP. STAT. 5/29D-14.9 (2016).
[190] Charles, *supra* note 188.
[191] FTC v. Kochava, 715 F. Supp. 3d 1319, 1324 (D. Idaho 2024).
[192] Carballo, Schmall & Tumin, *supra* note 48.
[193] *Id.*
[194] *See* Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898, 912 (S.D. Cal. 2020) ("[D]istrict courts have found that out-of-pocket expenses are sufficient to confer standing in data breach cases."); Pruchnicki v. Envision Healthcare Corp., 439 F. Supp. 3d 1226, 1236 (D. Nev. 2020), *aff'd,* 845 F. App'x 613 (9th Cir. 2021) (holding that damages stemming from lost time or emotional distress are not sufficient damages).
[195] 42 U.S.C. § 2000e(k).
[196] *See* NAACP v. Ala. *ex rel.* Patterson, 357 U.S. 449, 462 (1958).
[197] *Id.* at 466.
[198] *See* David A. Anderson, *Reputation, Compensation and Proof*, 25 WM. & MARY L. REV. 747, 748 (1984) (citing Charles T. McCormick, *The Measure of Damages for Defamation*, 12 N.C.L. REV. 120, 127 (1934)):

> [T]he plaintiff is relieved from the necessity of producing any proof whatsoever that he has been injured. From the fact of the publication of the defamatory matter by the defendant, damage to the plaintiff is said to be "presumed," and the jury, without any further data, is at liberty to assess substantial damages, upon the

directly overlaps with that of other areas of protected privacy.[199] One area of defamation is that of falsely claiming that a person has a "loathsome" disease.[200] The same harm to the person occurs if truthful information about having a "loathsome" disease is released without consent in a breach of confidentiality.[201] The disclosure itself is the harm because it increases the possibility that the individual will be treated differently by third parties, interfering with the individual's right of self-realization.

IV. HOW SHOULD THE LAW HANDLE DATA BREACHES OF PRIVATE INFORMATION THAT DO NOT INVOLVE OUT-OF-POCKET LOSSES?

Where a business's inadequate cybersecurity results in unauthorized access to private information, the individual's loss of control over that information should be viewed as a per se harm eligible for damages even when the individual has not yet suffered economic losses, and might never do so. A business can avoid liability by showing that it took reasonable steps to secure its network against unauthorized access.[202]

Our approach extends to any type of data that is sufficiently important to the "boundary regulatory process [by which] we regulate our accessibility to others."[203] We put aside considering what types of data meet this condition. Some may suggest that the European Union has already addressed the issue. The General Data Protection Regulation ("GDPR") Article 52 requires data controllers and processors to take "appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate."[204] Article 82 provides that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive

---

> assumption that the plaintiff's reputation has been injured and his feelings wounded.

[199] *See* RESTATEMENT (SECOND) OF TORTS § 652D (A.L.I. 1979) (stating that publicity of private facts is an invasion of privacy, creating liability under the common law tort of publicity given to private life).
[200] *Id.* § 572.
[201] *See id.* § 652D.
[202] The European Union takes a similar approach in the General Data Protection Regulation. *See, e.g.*, General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) (EU), at art. 82(2) [hereinafter GDPR], https://gdpr-info.eu/art-82-gdpr [https://perma.cc/FC8Z-NG46] ("A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."). The UK also has similar regulations in place. *See A Guide to Data Security*, IOC., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ [https://perma.cc/KLL4-ECUR].
[203] NIPPERT-ENG, *supra* note 152, at 22.
[204] GDPR, *supra* note 202, at art. 32.

compensation from the controller or processor for the damage suffered."[205] Does the concept of non-material damage cover a broad range of data important to the boundary regulatory process? That is unclear.[206]

In *UI v. Österreichische Post AG*, the European Union Court of Justice notes that the GDPR does not define the concept of non-material damage,[207] and it holds that Article 82 "confines itself to expressly stating that not only 'material damage' but also 'non-material damage' may give rise to a right to compensation, without any reference being made to any threshold of seriousness."[208] On the other hand, *AT, BT v. PS GbR, VG, MB, DH, WB, GS* held that

> a mere allegation of fear, with no proven negative consequences, cannot give rise to compensation under that provision. . . . Article 82(1) of the GDPR must be interpreted as meaning that a person's fear that his or her personal data have, as a result of an infringement of that regulation, been disclosed to third parties, without it being possible to establish that that was in fact the case, is sufficient to give rise to a right to compensation, provided that that fear, with its negative consequences, is duly proven.[209]

23andMe users allege fear of an increased risk of harm,[210] for which, on our proposal, they may recover without proof that the risk was realized. Consider *Thomas Bindl v. European Commission*, which found a compensable non-material harm when a transfer of information to the United States put Bindl "in a position of some uncertainty as regards the processing of his personal data, in particular of his IP address."[211] On the other hand, *BL v. MediaMarktSaturn Hagen-Iserlohn GmbH* held that "a purely hypothetical risk of misuse by an unauthorised third party cannot give rise to compensation. This is so where no third party became aware of the personal data at issue."[212] Our approach to an increased but non-imminent risk of harm includes such a hypothetical risk. We ground our approach in an emphasis on

---

[205] *Id.* at art. 82.
[206] *See* Case C-300/21, UI v. Österreichische Post AG, ECLI:EU:C:2023:370, ¶ 45 (May 4, 2023); *but see* Case C-590/22, AT, BT v. PS GbR, VG, MB, DH, WB, GS, C-590/22, ECLI:EU:C:2024:536, ¶¶ 35–36 (June 20, 2024).
[207] Case C-300/21, UI v. Österreichische Post AG, ECLI:EU:C:2023:370, ¶ 30.
[208] *Id.* ¶ 45.
[209] Case C-590/22, AT, BT v. PS GbR, VG, MB, DH, WB, GS, ECLI:EU:C:2024:536, ¶¶ 35–36.
[210] *See, e.g.,* Complaint at 15, *In re* 23andMe, Inc., Customer Data Sec. Breach Litig., No. 24-md-03098.
[211] Case T-354/22, Thomas Bindl v. European Commission, ECLI:EU:T:2025:4, ¶ 197 (Jan. 8, 2025).
[212] Case C-687/21, BL v. MediaMarktSaturn Hagen-Iserlohn GmbH, ECLI:EU:C:2024:72, ¶ 68 (Jan. 25, 2024).

the "boundary regulatory process [by which] we regulate our accessibility to others"[213] and believe this provides more guidance than the GDPR currently does.[214]

V. CONCLUSION

We advocate that courts and legislatures recognize the harms that flow from the loss of control of sensitive private information in a data breach. They should compensate individuals even when they do not suffer out-of-pocket losses in order to deter entities from insufficiently protecting such information. The power to regulate to whom and what type of private information is revealed is central to our ability to define ourselves and to protect ourselves against harm. Common law, statutory law, constitutional law—and underlying psychological truths about self-realization—provide ample precedents for such an approach.[215]

---

[213] NIPPERT-ENG, *supra* note 152.
[214] *See* GDPR, *supra* note 202.
[215] *See* Anderson, *supra* note 198, at 748; OR. REV. STAT. § 192.541 (2023); NAACP v. Ala. *ex rel.* Patterson, 357 U.S. 449, 462 (1958).