

In this issue:

- 4. Writing Prompts to Identify At-Risk Students in Introductory Programming Courses**  
Jon D. Clark, Colorado State University  
Seth J. Kinnett, Colorado State University
  
- 16. When One Account Exposes Millions: Design Debt, Relational Exposure, and the 23andMe Breach**  
David J. Yates, Bentley University  
Arthur Ream III, Bentley University
  
- 32. Implementing Personalized Learning Pathways as Informed by the 5E Model: Digital Tools to the Rescue!**  
Celeste Tipple, LaTrobe University  
Tanya Linden, The University of Melbourne
  
- 48. How 21st Century Skills Have Evolved in the 21st Century and How AI Is Shaping Their Next Evolution**  
Mark Frydenberg, Bentley University  
Kevin Mentzer, Nichols College
  
- 62. Teaching Case**  
**Paddles for Paws: Development of a Pickleball Tournament Event Management Database for a Cool Cause**  
Dana Schwieger, Southeast Missouri State University
  
- 75. Teaching Case**  
**From Concept to Canvas: Leveraging Generative AI to Co-Design Business Visuals**  
Fang Chen, University of Montana  
Bryan Hammer, University of Montana  
Shawn Clouse, University of Montana  
Patricia Akello, University of Montana

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is five times per year. The first year of publication was 2003.

ISEDJ is published online (<https://isedj.org>). Our sister publication, the Proceedings of the ISCAP Conference (<https://iscap.us/proceedings>) features all papers, abstracts, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. All papers, whether award-winners or not, are invited to resubmit for journal consideration after applying feedback from the Conference presentation. Award winning papers are assured of a publication slot; however, all re-submitted papers including award winners are subjected to a second round of three blind peer reviews to improve quality and make final accept/reject decisions. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is under 35%.

Information Systems Education Journal is pleased to be listed in the Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at [editor@isedj.org](mailto:editor@isedj.org) or the publisher at [publisher@isedj.org](mailto:publisher@isedj.org). Special thanks to volunteer members of ISCAP who perform the editorial and review processes for ISEDJ.

### 2026 ISCAP Board of Directors

Amy Connolly  
James Madison University  
President

Michael Smith  
Georgia Institute of Technology  
Vice President

Jeff Cummings  
Univ of NC Wilmington  
Past President

David Firth  
University of Montana  
Director

Mark Frydenberg  
Bentley University  
Director/Secretary

Leigh Mutchler  
James Madison University  
Director

RJ Podeschi  
Millikin University  
Director/Treasurer

Bryan Reinicke  
Rochester Institute of  
Technology / Director

Jeffrey Babb  
West Texas A&M University  
Director/Curricular Matters

Eric Breimer  
Siena University  
Director/2026 Conf Chair

Thomas Janicki  
Univ of NC Wilmington  
Director/Meeting Planner

Xihui "Paul" Zhang  
University of North Alabama  
Director/JISE Editor

Copyright © 2026 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Kevin Mentzer, Editor, [editor@isedj.org](mailto:editor@isedj.org).

# INFORMATION SYSTEMS EDUCATION JOURNAL

## Editors

---

**Kevin Mentzer**  
Editor  
Nichols College

**Ira Goldman**  
Associate Editor  
Siena University

**David Yates**  
Associate Editor  
Bentley University

**Michelle Louch**  
Teaching Cases & Exercises  
Editor  
University of Pittsburgh - Greensburg

**Mark Pisano**  
Teaching Cases & Exercises  
Associate Editor  
Southern Connecticut  
State University

**Thomas Janicki**  
Publisher  
Univ of NC Wilmington

**David Woods**  
Assistant Publisher  
Miami University  
Regionals

**Paul Witman**  
Emeritus Editor  
(2021-2026)  
California Lutheran  
University

**Jeffry Babb**  
Emeritus Editor  
(2016-2021)  
West Texas A&M  
University

**Donald Colton**  
Emeritus Editor  
(2003-2010)  
Brigham Young University  
Hawaii

# When One Account Exposes Millions: Design Debt, Relational Exposure, and the 23andMe Breach

David J. Yates  
dyates@bentley.edu

Arthur Ream III  
areamiii@bentley.edu

Department of Computer Information Systems  
Bentley University  
Waltham, MA 02452, USA

## Abstract

This case examines the 2023 breach of 23andMe to illustrate how accumulated design debt in a relational genetic platform produced a condition of privacy fragility, enabling the compromise of 14,000 accounts to expose profile data from 6.9 million users. Rather than a traditional security failure, the incident reveals how architectural choices – visibility defaults, optional authentication safeguards, and weak consent mechanisms – can amplify harm across genetically linked networks. The case traces the breach’s escalation, the company’s delayed and defensive response, and the governance and legal challenges that culminated in 23andMe’s 2025 bankruptcy and data transfer to a new corporate entity. Designed for one or two class sessions, the case offers a well-structured teaching case with conceptual scaffolding. It also offers instructors a foundation for discussing platform accountability in data-intensive systems. This case can be used in undergraduate courses in information systems, cybersecurity, or governance to anchor one or two class meetings on architectural trade-offs, privacy risk, digital platforms, and incident response.

**Keywords:** Privacy fragility, design debt, relational exposure, genetic data, cybersecurity breach, platform accountability

**Recommended Citation:** Yates, D.J., Ream III, A.F., (2026). When One Account Exposes Millions: Design Debt, Relational Exposure, and the 23andMe Breach. *Information Systems Education Journal*, v24(n3) pp 16-31. DOI# <https://doi.org/10.62273/TQZO9281>

# When One Account Exposes Millions: Design Debt, Relational Exposure, and the 23andMe Breach

David J. Yates and Arthur Ream III

## 1. INTRODUCTION

This manuscript is structured as an analytical teaching case intended for classroom use. It integrates technical breach mechanics with organizational governance, regulatory context, and structural design considerations. Sections 2–4 support architectural analysis; Sections 5–7 support governance and policy discussion. Instructors may assign selected sections independently or teach the full case across two sessions.

### Learning Objectives

After engaging with this case, students will be able to:

- Explain how architectural choices -- visibility defaults, authentication design, and consent mechanisms -- can produce conditions of privacy fragility in data-intensive platforms.
- Apply the concept of design debt to diagnose why 23andMe's post-incident remediation options were constrained.
- Distinguish relational privacy harms from individual privacy harms, and evaluate the adequacy of traditional consent frameworks in relational data systems.
- Analyze an organization's breach response against established frameworks such as NIST SP 800-61 Rev. 3 and Fair Information Practice Principles.
- Discuss the ethical, legal, and data stewardship implications of transferring biometric and genetic data during corporate bankruptcy.

### Target Audience and Prerequisites

The case is suitable for upper-division undergraduate courses in information systems, cybersecurity, IT (or data) governance, or digital platforms. Familiarity with basic cybersecurity concepts and introductory data privacy law is helpful but not required; the necessary context is provided within the case.

### Suggested Teaching Plan

**Session 1 (Sections 2–4):** Breach mechanics and architectural analysis. Open with discussion of the *DNA Relatives* feature and how network design shapes the attack surface. The discussion prompts (Section 8) help anchor this session.

**Session 2 (Sections 5–7):** Impact, governance, and policy. Focus on legal gaps, leadership accountability, design debt as a governance constraint, and data stewardship during bankruptcy. Discussion prompts also help anchor this session.

### Suggested Student Deliverables (Optional)

- A policy memo recommending mandatory cybersecurity controls for direct-to-consumer genetic platforms.
- A redesign proposal for the DNA Relatives consent architecture that addresses second-order data subjects.
- A comparative analysis of 23andMe's breach response against a chosen incident response framework.

Instructors seeking sample discussion answers are encouraged to contact the corresponding author directly.

## 2. KEY CONCEPTS: RELATIONAL ARCHITECTURE, DESIGN DEBT, AND PRIVACY FRAGILITY

This paper uses three interlocking constructs -- relational architecture, design debt, and privacy fragility -- in specific ways. Because these terms are not used here in entirely standard fashion, brief definitions are provided before the case analysis.

### Relational Architecture

In information systems research, *relational* most often refers to relational database management systems in which data is organized into tables linked by primary and foreign keys (Codd, 1970). That is not the meaning used here. In this paper, *relational* refers to a platform-level condition in which user accounts are structurally connected through shared data, inferred ties, or visibility mechanisms such that the exposure of one account can alter the privacy surface of others.

A relational architecture therefore creates persistent, traversable connections among users. DNA Relatives exemplified this condition. Each user who opted in became a node in a network, while the ties between nodes -- shared genetic segments, match scores, and related profile

information -- could be explored through the platform's interface. In a non-relational design, breaching Account A primarily exposes Account A's data. In a relational design, breaching Account A may also expose information about users reachable through the linkage structure. The extent of amplification depends on graph density, the granularity of visible attributes, and the presence or absence of containment mechanisms.

### **Design Debt**

The concept of technical debt, introduced by Cunningham (1992), describes the future costs created when developers adopt expedient solutions instead of more robust ones. *Design debt* is a broader construct. It refers to the deferred costs associated with architectural, interaction-design, or policy-design decisions whose risks may remain latent until a system scales, threats evolve, or a failure occurs (Kruchten, Nord & Ozkaya, 2012; Avgeriou et al., 2016). Unlike narrow code-level debt, design debt concerns how a system is structured, how users encounter and manage risk, and how data flows are governed over time.

At 23andMe, the most consequential debt was architectural and policy-based rather than code-level. The company did not require MFA by default, allowed DNA Relatives to operate with broad visibility, and relied on consent mechanisms centered on direct participants rather than indirectly affected relatives. Each decision may have reduced friction and supported growth, but each also deferred risk. Over time, these choices increased authentication exposure, widened relational visibility, and limited the company's ability to respond effectively once the breach occurred.

### **Privacy Fragility**

Privacy fragility describes a condition in which a limited failure produces privacy harm across a much larger population (Kotlan, Magoon & Yates, 2026). It emerges when three conditions coincide: A densely connected relational architecture, weak containment mechanisms, and a breach or misuse event. The 23andMe case illustrates this dynamic: Once accounts were linked through DNA Relatives, the compromise of a small set of credentials exposed far more than the directly accessed accounts. This concept parallels systemic fragility in other domains: Systems may appear manageable under normal conditions yet fail non-linearly once a threshold is crossed (Minsky, 1986; Woods, 2015).

### **Relational Privacy**

Relational privacy builds on Nissenbaum's (2004)

theory of contextual integrity and emphasizes that, in some environments, information about one person is also information about others. This is especially true in genetic systems, genealogical databases, and family health records. As Phillips (2016) argues, such contexts create involuntary data subjects: Individuals whose privacy may be affected not by their own choices, but by the participation of relatives. Traditional consent models, which assume that privacy decisions are individualized and self-contained, are poorly suited to these circumstances unless they are adapted to account for indirect and second-order exposure.

### **3. 23andMe AND THE DNA RELATIVES FEATURE**

Founded in 2006, 23andMe became one of the leading direct-to-consumer (DTC) genetic testing platforms by offering ancestry and health-related insights derived from user-submitted saliva samples (Regalado, 2019). By 2022, the company had collected genetic data from more than twelve million customers and had expanded its revenue model through partnerships and data-driven drug discovery. That scale made the platform commercially significant, but it also increased the importance of security, privacy, and governance.

A defining feature of the platform was DNA Relatives, an opt-in service that enabled users to identify and connect with genetically similar individuals in the database. The feature supported genealogical discovery and user engagement, but it also created relational exposure. Because genomic data is inherently shared across biological networks, one person's participation could reveal identity cues or probabilistic traits about relatives who had never joined the platform or opted into the feature. DNA Relatives therefore did more than expose individual profile data; it transformed participation into a source of visibility for others linked through genetic similarity.

The platform's privacy posture compounded this dynamic. 23andMe's Privacy Statement permitted the collection of extensive genetic, demographic, and behavioral information and allowed the company to revise its policies over time. Although aggregate or research datasets were often described as anonymized, prior research has shown that genomic data can sometimes be re-identified when combined with auxiliary information (Bampoulidis & Lupu, 2019). These technical and policy choices meant that 23andMe was not simply storing isolated customer records.

It was building an expanding graph of linked identities, profiles, and inferences.

That architecture became especially consequential in late 2023, when attackers used credentials recycled from breaches elsewhere to access approximately 14,000 23andMe accounts. Because many of those accounts were enrolled in DNA Relatives, the attackers were able to view profile information associated with roughly 6.9 million additional users. What began as credential-based account compromise expanded through the platform's relational design. A feature intended to facilitate discovery and connection thus amplified the consequences of a relatively limited authentication failure by allowing exposure to propagate across a much larger visibility network.

23andMe initially emphasized password reuse as the primary cause of the incident, but that explanation was incomplete. By focusing on user behavior, the company downplayed the role of optional two-factor authentication, limited automated login monitoring, and visibility settings that enabled secondary exposure within DNA Relatives. Privacy scholars and cybersecurity analysts argued that the platform's relational architecture, combined with weak containment safeguards, materially magnified the scale of harm (Holthouse, Owens & Bhunia, 2025; 23andMe, 2024).

The case is therefore more than an example of credential stuffing. It demonstrates how platform design and governance choices shaped both the attack surface and the downstream consequences of failure. DNA Relatives enhanced engagement and personalized discovery, yet it also externalized privacy risk to relatives, weakened the adequacy of individualized consent, and amplified the effects of authentication compromise. In this sense, the breach was not simply the result of reused passwords. It was also the product of accumulated design debt embedded in a relational architecture that made systemic exposure possible. Once a relatively small number of accounts were compromised, privacy harm propagated across a densely connected visibility graph, affecting many individuals who had never meaningfully chosen to participate in that exposure.

#### **4. CREDENTIAL STUFFING ATTACK AND SCOPE OF EXPOSURE**

In October 2023, 23andMe confirmed that the breach began with a credential-stuffing attack that compromised approximately 14,000

accounts. Credential stuffing uses previously leaked username-password combinations to gain access to accounts on unrelated platforms, and is particularly effective when multi-factor authentication (MFA) is optional and high-volume login attempts are not monitored -- both conditions present on 23andMe's platform at the time (Holthouse, Owens & Bhunia, 2025).

The breach rapidly expanded because compromised accounts acted as gateways into millions of additional profiles through the DNA Relatives feature. Many of the 14,000 directly breached users had opted into DNA Relatives, which displays genealogical matches and profile attributes from other users; as a result, the attacker could view data linked to about 6.9 million individuals (23andMe, 2024). This expansion occurred without any deeper intrusion into 23andMe's internal systems, illustrating how the platform's relational design magnified the consequences of weak authentication.

The attacker obtained access to highly identifiable genetic and demographic information, including ancestry results, haplogroups, inferred family relationships, names, photos, geographic indicators, and user-submitted traits. Although some data elements were nominally non-identifying, prior research shows that genetic data can often be re-identified when paired with auxiliary datasets or publicly available information (Gymrek et al., 2013; Erlich & Narayanan, 2014).

The company's initial public response centered on the narrative that the incident resulted from user password reuse rather than platform shortcomings. While 23andMe noted that its systems had not been hacked, this framing overlooked structural vulnerabilities -- such as optional MFA, insufficient rate-limiting, and absent anomaly detection -- even though predictable user behaviors like password reuse are well-documented in the security-usability literature (Florêncio & Herley, 2010).

The breach took on new dimensions when the attacker began selling ethnicity-specific datasets extracted from the compromised profiles. These included data on more than one million Ashkenazi Jewish users and over 100,000 users of Chinese descent (Carballo, Schmall & Tumin, 2024). The emergence of these curated datasets raised concerns about discrimination, stigmatization, and targeted surveillance, underscoring how genetic information can be exploited for harmful population-level inference.

At a technical and governance level, the incident revealed multiple systemic failures in 23andMe's security and privacy architecture. MFA was not mandated despite the sensitivity of the underlying data; rate-limiting and automated detection mechanisms did not prevent bulk login attempts; and users were not fully informed that their DNA Relatives participation could expose others. These weaknesses reflected a broader misalignment between the permanence and relational nature of genetic data and the comparatively modest safeguards applied to it.

Regulatory and legal responses accelerated because millions of individuals who had never opted into DNA Relatives were nonetheless exposed through relatives who had participated, raising novel questions about relational consent and platform accountability (Gerke, Jacoby & Cohen, 2025). State attorneys general opened investigations and affected users brought class-action lawsuits citing deceptive practices and inadequate cybersecurity protections (23andMe, 2024; Hernandez, 2025; Kirk, 2025).

### **5. IMMEDIATE RESPONSE: COMMUNICATIONS, REMEDIATION, AND GOVERNANCE BREAKDOWN**

23andMe's initial reaction to the breach drew criticism because the company framed the incident as a matter of user misconduct rather than platform vulnerability. In its October 6, 2023, announcement, the firm emphasized that its systems had not been "hacked" and attributed the breach to users reusing passwords from prior incidents (23andMe, 2024). This framing deflected responsibility, even though predictable password reuse is well documented in the security-usability literature (Florêncio & Herley, 2010).

Public confidence eroded further because the company relied on staggered, delayed disclosures rather than timely, comprehensive notification. 23andMe did not file a breach notice with the California Attorney General until January 2024, months after signs of suspicious activity first emerged (23andMe, 2024). Although the company cited investigative complexity, the delay raised broader concerns about its preparedness to manage sensitive, large-scale genetic data (Hernandez, 2025).

When the company did implement remediation, 23andMe required password resets without mandating multi-factor authentication, undermining the utility of its primary security response. Optional 2FA had long been a structural

vulnerability, and its continued optionality after the breach ignored the uniquely sensitive, immutable nature of the affected genetic and relational data. These response limitations reflect accumulated design debt rather than isolated implementation failures.

The incident also revealed that internal and external governance mechanisms failed across multiple layers of the response. Internally, there was no evidence of a formal incident response program aligned with frameworks such as NIST SP 800-61 Rev. 3 (Nelson et al., 2025). Externally, the company delayed communication not only with regulators but also with research partners and millions of indirectly affected users. By the time formal notices were issued in January 2024, compromised datasets were already circulating on dark web markets.

In communications to users, 23andMe adopted a minimization strategy that overlooked the platform's relational exposure architecture. The company emphasized that only users who reused passwords were directly compromised and that DNA Relatives participation was voluntary (23andMe, 2023). This narrative sidestepped the fact that many individuals exposed through DNA Relatives had not opted into the feature themselves, as later alleged in multiple lawsuits (Kirk, 2025). These second-order harms challenge traditional notions of consent (Nissenbaum, 2004) and demonstrate the limitations of identity-based legal definitions of personal data (Schwartz & Solove, 2011).

Remediation was further weakened because 23andMe did not individually notify users whose information was exposed indirectly through relatives, creating a gap between the affected population and those who received assistance. Although the company offered credit monitoring to a subset of users, it did not extend support to the millions of relatives affected indirectly – a stance inconsistent with modern Fair Information Practices (Gellman, 2025) and regulatory expectations under frameworks such as the GDPR (Greenleaf, 2011; Shabani & Borry, 2018).

Public trust deteriorated even further because the company's leadership remained largely silent throughout the crisis, despite its branding as an ethics-conscious, science-forward organization (Carballo, Schmall & Tumin, 2024; Rutherford, 2025). CEO Anne Wojcicki did not make a substantive public statement until months after the breach and ultimately did not testify before Congress until June 2025.

The company's crisis management also revealed that regulatory gaps and permissive platform policies enabled weak accountability during the response. This regulatory ambiguity became more problematic as 23andMe approached bankruptcy and asset transfer, where contractual consent superseded meaningful user control (Gerke, Jacoby & Cohen, 2025).

Under growing public and legal pressure, 23andMe eventually issued an action plan promising stronger authentication, expanded auditing, and more granular consent controls, but these commitments were voluntary, limited, and widely viewed as oriented toward litigation and public-relations management rather than deeper institutional reform (23andMe, 2023).

In the months that followed, the company faced mounting litigation, multi-state investigations, and regulatory attention across the U.S., U.K., and EU, yet it remained largely shielded by its Terms of Service – highlighting how contractual consent can displace substantive privacy protections when statutory safeguards are weak.

In short, 23andMe's response was delayed, defensive, and structurally incomplete, obscuring architectural contributors to the breach and failing to meet expectations of transparency, preparedness, and ethical stewardship (Barocas & Nissenbaum, 2009). This phase of the incident illustrates how minimization rhetoric and insufficient crisis governance can amplify reputational, legal, and operational damage long after the initial compromise.

## **6. IMPACT ASSESSMENT: DATA BREACH SCALE, SENSITIVE DATA AT RISK, AND LEGAL/FINANCIAL FALLOUT**

The breach revealed that a small number of compromised accounts created an outsized privacy disaster because platform design amplified the scale of exposure. Although the attacker directly accessed roughly 14,000 accounts through credential stuffing, the structure of DNA Relatives allowed the scraping of data from approximately 6.9 million users (23andMe, 2024; Lanzing, 2016; Holthouse, Owens & Bhunia, 2025). This was not the result of malware or database intrusion, but of architectural choices that failed to contain relational visibility, dramatically expanding the breach's long-term consequences.

The compromised dataset demonstrated that the breach exposed highly sensitive, uniquely permanent biometric and familial information.

Names, ancestry results, haplogroups, inferred relationships, photographs, locations, and shared DNA segments were all accessible – attributes that cannot be revoked or changed (Erich & Narayanan, 2014; 23andMe, 2023, 2024, n.d.). Genomic data also gains value over time because of its predictive, inferential, and relational characteristics, meaning harms can extend to relatives and descendants (Narayan, Kohli & Martin, 2025).

The incident escalated into a legal and regulatory crisis because millions of individuals who never opted into DNA Relatives were exposed through those who did, revealing deep flaws in traditional consent models. Class-action lawsuits filed in early 2024 argued deceptive practices and negligent protection of sensitive data, emphasizing the exposure of individuals who had made no affirmative disclosure decisions (Kirk, 2025). This highlighted the inadequacy of consent centered solely on individual users in contexts where data is inherently shared.

Across jurisdictions, regulators responded because the breach violated emerging expectations for safeguarding special-category data and transparency in high-risk systems. The U.K. ICO imposed a £2.31 million GDPR fine for inadequate organizational and technical protections, and investigations by U.S. and Canadian regulators soon followed. The FTC raised concerns under Section 5, particularly regarding privacy promises and the downstream transfer of genetic data during bankruptcy (Lee, 2025).

Legal remedies remained limited because U.S. privacy law does not yet recognize relational privacy or second-order data subjects, leaving large categories of affected individuals without formal recourse. A \$30 million preliminary settlement in 2024 covered only directly compromised users, excluding relatives whose data became exposed through DNA Relatives (Hernandez, 2025). Privacy scholars have noted that such omissions reflect structural gaps in the U.S. regulatory landscape (Nissenbaum, 2004; Schwartz & Solove, 2011).

Financially, the breach accelerated 23andMe's decline and contributed to the company's eventual bankruptcy. Once valued at roughly \$3.5B at IPO, 23andMe's stock fell below \$1 by 2023 and the firm entered Chapter 11 in March 2025 (Greely, 2020; Hernandez, 2025); see Appendix B. At the time of filing, market capitalization had fallen to under \$50 million -- approximately 1.4% of its IPO valuation --

reflecting the combined reputational, legal, and operational damage wrought by the breach and its aftermath. By then, the company held genetic data from over 15 million users and had accumulated over \$300 million in losses.

The bankruptcy process intensified concerns because genetic data held by distressed firms can become a commercial asset with limited statutory protections. Although 23andMe's privacy statement claimed that user data would not be sold without consent, it also reserved the right to transfer information during corporate restructuring, creating a contradiction that surfaced during bankruptcy auctions (23andMe, n.d.; Bradshaw, Millard & Walden, 2011). As Gerke, Jacoby, and Cohen (2025) note, U.S. bankruptcy law offers only weak safeguards for sensitive personal data.

These tensions came to a head when Anne Wojcicki repurchased the company's assets – including its genetic database – through the TTAM Research Institute, outbidding firms such as Regeneron (Saey, 2025; Kirk, 2025). Privacy advocates questioned whether legacy user consent extended to post-bankruptcy transfers, especially given the company's history of privacy policy revisions without explicit re-consent (Gellman, 2025).

The fallout extended beyond legal and financial impacts because the breach triggered a significant erosion of public trust in direct-to-consumer genetic testing. Media reports documented rising numbers of users deleting profiles, downloading data, or abandoning the platform altogether (Saey, 2025; Rutherford, 2025). Many found that withdrawal was constrained by retention policies and longstanding research agreements.

The 23andMe journey unfolded to produce a state of privacy fragility in which the compromise of one account could expose entire familial networks (Boyd & Crawford, 2012; Phillips, 2016).

The aftermath of the 23andMe breach has already prompted calls for:

- stronger breach notification rules that include indirect victims;
- clearer restrictions on genetic data transfers during bankruptcy; and
- greater platform accountability for relational exposure risks.

## **7. POST-INCIDENT GOVERNANCE: ACCOUNTABILITY, ACQUISITION, AND DATA STEWARDSHIP**

The post-incident phase made clear that 23andMe's governance breakdown was not simply a matter of weak crisis communication or isolated managerial error. It reflected constraints created by years of design choices that prioritized growth, visibility, and engagement over containment, user control, and accountability. By the time the company was responding to the breach, its relational architecture linked profiles through DNA Relatives, relied on weak consent structures, and offered limited mechanisms for retroactive protection. As litigation mounted and bankruptcy approached, these constraints interacted with leadership silence and regulatory gaps, turning a security incident into a broader failure of stewardship.

Throughout 2024, 23andMe's board and senior leadership did not provide a full public accounting of the breach or the factors that amplified it. CEO Anne Wojcicki made only limited public comments, and no senior executive testified before Congress or major regulators about incident handling until June 2025 (Rutherford, 2025). The company also did not publish a detailed independent breach report or commission a third-party audit. This lack of transparency drew criticism from privacy advocates and investors, who argued that the company treated genetic data governance as a matter of proprietary control rather than public trust. In a platform built on sensitive and enduring user data, the absence of visible internal reform weakened confidence that the company understood the harm or its stewardship obligations.

Weak accountability was reinforced by the legal environment in which 23andMe operated. Consumer genetic data in the United States remained subject to a patchwork of protections, and the company's Terms of Service explicitly permitted transfers of user data during mergers, acquisitions, or bankruptcy. That clause became central once 23andMe entered financial distress and its assets, including its genomic database, were put up for sale. In June 2025, TTAM Research Institute, a new entity created by Wojcicki, won the auction for 23andMe's assets in a \$305 million deal, outbidding firms including Regeneron Pharmaceuticals (Saey, 2025; Kirk, 2025; Herper, 2025). Although the transaction promised continuity for users and research partnerships, it also raised difficult questions about whether earlier consent agreements, often

accepted under prior privacy policies and narrower expectations, could authorize the transfer of sensitive biometric and relational data to a new entity.

Those concerns were intensified by the lack of any broad-based re-consent process before or after the sale. Privacy scholars have long argued that consent in high-risk data environments cannot be treated as a one-time contractual event divorced from context, organizational change, and downstream use. Yet 23andMe's governance posture largely assumed that legacy terms were sufficient. The result was a weak form of accountability in which continuity promises substituted for renewed user authorization, even though the company's ownership structure, financial condition, and trust posture had changed dramatically.

The breach also demonstrated how accumulated design debt narrowed the range of post-incident responses. DNA Relatives created value for users, but it did so by making relational linkages broadly visible and by offering limited safeguards against secondary exposure. Broad profile sharing, insufficiently granular privacy controls, and the lack of conservative default settings made it difficult to stop cascading exposure or restore privacy expectations after the breach. Even after the incident, 23andMe did not introduce mechanisms that would allow users to control how their information appeared in others' match results or to retract already shared relational data. Instead, optional and relatively hidden settings continued to reflect a design philosophy that externalized familial risk. Once millions of users had been connected through the platform's visibility structure, those relationships could not be easily unwound.

The bankruptcy and transfer to TTAM therefore raised a question: Who should be trusted to steward one of the world's largest consumer genetic databases after a governance failure? Although 23andMe's privacy policy stated that personal information would not be sold without consent, it also treated data as transferable during restructuring, effectively allowing sensitive genetic information to move as part of an asset sale. With TTAM, led by the company's former CEO, assuming custodianship, users were left to rely largely on assurances of continuity rather than enforceable, updated permissions. Because 23andMe had revised its privacy policies multiple times without requiring explicit re-consent from legacy users, many individuals now face the prospect that their genetic information is governed by terms they may never have

reviewed or accepted.

Taken together, these post-incident dynamics show that the 23andMe breach evolved into more than a case of poor cybersecurity. It became a test of whether institutions that collect persistent, relational, and sensitive data can remain accountable when technical failure, legal ambiguity, and organizational distress occur at the same time. Years of accumulated design debt left 23andMe with little room to maneuver after the breach, while contractual consent and bankruptcy law allowed its data assets to remain transferable despite questions about legitimacy, user expectation, and long-term stewardship. The case therefore illustrates how leadership silence, technical lock-in, and weak legal safeguards can converge to limit meaningful accountability after a major platform failure.

## **8. DISCUSSION, LIMITATIONS, AND CONCLUDING REMARKS**

### **Discussion**

The 23andMe breach shows that failures in data-intensive platforms are often structural as well as technical. Reused passwords opened the door, but the scale of harm was shaped by platform design: DNA Relatives converted individual accounts into points of access for genetically linked others, while weak authentication, limited containment, and permissive data-governance terms magnified downstream exposure. The result was not simply a breach of 14,000 accounts, but a broader failure of stewardship over persistent, biometric, and relational data.

The case reinforces three broader implications. First, platforms handling relational data cannot rely on user choice alone, because one person's participation may expose others who never meaningfully consented. Second, privacy harms in these environments are networked rather than isolated: A small failure can cascade across many profiles when visibility and linkage are built into the system. Third, design debt matters because architectural and policy choices made for growth, usability, or engagement can later limit response options when a crisis occurs. In 23andMe's case, the company could not easily unwind relational visibility, restore prior privacy expectations, or separate routine product functionality from systemic exposure once the breach occurred.

Several governance lessons follow. Accountability cannot be outsourced to users. Blaming password reuse overlooks predictable behaviors and understates the platform's responsibility to require stronger authentication, detect

anomalous access, and constrain unnecessary visibility (Florêncio & Herley, 2010; Holthouse, Owens & Bhunia, 2025). Relational data also requires relational governance. Where system outputs affect people beyond the direct user, governance must account for second-order data subjects, indirect exposure pathways, and collective harm (Narayan, Kohli & Martin, 2025). In addition, contractual permission is not the same as ethical legitimacy. Terms allowing transfer during merger or bankruptcy may satisfy formal notice requirements while still violating user expectations for sensitive genetic and biometric data (Bradshaw, Millard & Walden, 2011). Finally, leadership transparency remains central to trust. Delayed acknowledgment, defensive framing, and limited executive visibility can deepen institutional damage long after the initial compromise (Rutherford, 2025).

### Suggested Discussion Prompts

These prompts are designed for use in undergraduate information systems, cybersecurity, IS security, and IT (or data) governance courses.

- How could 23andMe have redesigned DNA Relatives to reduce relational exposure without sacrificing functionality?
- What mandatory cybersecurity controls make sense for biometric/relational data (e.g., MFA-by-default, rate-limiting, anomaly detection); how would you evaluate their effectiveness?
- How does design debt shape the feasibility of post-incident reforms?
- Under what conditions should platforms be permitted to transfer biometric data during bankruptcy, and what constraints should apply?

These lessons should be understood alongside the incentives 23andMe faced. Features such as DNA Relatives supported engagement, differentiation, and network effects in a competitive market, while stricter authentication and narrower visibility likely would have introduced friction. Those trade-offs help explain the platform's trajectory, but they do not diminish responsibility for failing to anticipate how relational exposure, once embedded, could scale harm so rapidly.

### Limitations

This analysis has several limitations. First, individuals exposed indirectly through genetic linkages received limited recognition in litigation and regulation, leaving an incomplete empirical record of second-order harm (Calo, 2011;

Schwartz & Solove, 2011; Carballo, Schmall & Tumin, 2024). Second, although 23andMe announced new security and consent measures, those changes do not appear to provide retroactive visibility controls or meaningful ways to reclaim already-shared data (23andMe, 2023). Third, TTAM Research Institute has signaled a public-interest orientation, but its long-term governance model remains uncertain, and no broad re-consent process has been launched (Herper, 2025). Future research should examine whether these commitments produce enforceable protections in practice.

### Concluding Remarks

The 23andMe breach illustrates how design debt in relational systems can harden into privacy fragility. Once broad visibility, weak consent structures, and permissive transfer terms become embedded in a platform, a relatively small compromise can expose far larger populations, while remediation choices narrow sharply (Erich & Narayanan, 2014; Hernandez, 2025; Kotlan, Magoon & Yates, 2026). For that reason, this breach should be understood not as an anomaly, but as an early warning about the behavior of biometric and inferential data systems under stress.

For scholars, practitioners, and students, the central lesson is that protecting relational and biometric data requires more than better passwords, stronger MFA, or improved incident response. It also requires governance models that treat consent as ongoing and contextual, recognize second-order data subjects, and impose substantive limits on data reuse and transfer, especially during restructuring and bankruptcy. As more platforms collect genetic, biometric, and behavioral traces, the 23andMe case offers a clear warning: Systems built for connection and growth can also concentrate long-term, distributed harms when their governance fails.

## 9. REFERENCES

- 23andMe. (2018, Jul. 25). A Note On 23andMe's New Collaboration with GSK. <https://mediacenter.23andme.com/press-releases/23andme-and-gsk/>
- 23andMe. (2021, Jun. 17). 23andMe successfully closes its business combination with VG Acquisition Corp. <https://mediacenter.23andme.com/press-releases/23andme-closes-business-combination/>

- 23andMe. (2022, May 26). 23andMe reports FY2022 full-year financial results. <https://investor.23andme.com/news-releases/news-release-details/23andme-reports-fy2022-full-year-financial-results>
- 23andMe. (2023, Dec. 5). Addressing Data Security Concerns – Action Plan. <https://blog.23andme.com/articles/addressing-data-security-concerns>
- 23andMe. (2024, Jan. 22). Notice of data breach. *Office of The Attorney General*, Sacramento, CA. <https://oag.ca.gov/system/files/CA%20AG%20-%20CA%20Notification%20Letters.pdf>
- 23andMe. (n.d.). Legal – Privacy Statement. *23andMe*, San Francisco, CA, USA. <https://www.23andme.com/legal/privacy/full-version/>
- Avgeriou, P., Kruchten, P., Ozkaya, I., & Seaman, C. (Eds.). (2016). Managing technical debt in software engineering (Dagstuhl Seminar 16162). *Dagstuhl Reports*, 6(4), 110–138. doi:10.4230/DagRep.6.4.110
- Bampoulidis, A., & Lupu, M. (2019). *An abstract view on the de-anonymization process*. arXiv preprint. <https://doi.org/10.48550/arXiv.1902.09897>
- Barocas, S., & Nissenbaum, H. (2009). On Notice: The Trouble with Notice and Consent. In *Proceedings of the Engaging Data Forum*, Cambridge, MA.
- Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, 15(5), 662–679. <https://doi.org/10.1080/1369118X.2012.678878>
- Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, 19(3), 187–223. <https://doi.org/10.1093/ijlit/ear005>
- Calo, R. (2011). The Boundaries of Privacy Harm. *Indiana Law Journal*, 86(3), 1131–1161.
- Carballo, R., Schmall, E., & Tumin, R. (2024, Jan. 26). 23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says. *New York Times*. <https://www.nytimes.com/2024/01/26/business/23andme-hack-data.html>
- Codd, E. F. (1970). A relational model of data for large shared data banks. *Communications of the ACM*, 13(6), 377–387. <https://doi.org/10.1145/362384.362685>
- Cunningham, W. (1992). The WyCash portfolio management system. In *Addendum to the Proceedings of OOPSLA '92*. <https://doi.org/10.1145/157709.157715>
- Erlich, Y., & Narayanan, A. (2014). Routes for breaching and protecting genetic privacy. *Nature Reviews Genetics*, 15(6), 409–421. <https://doi.org/10.1038/nrg3723>
- Florêncio, D., & Herley, C. (2010). Where do security policies come from? In *Proc. of Symposium on Usable Privacy and Security*. <https://doi.org/10.1145/1837110.1837124>
- Gellman, R. (2025). Fair Information Practices: A Basic History (Version 2.32). *Center for Democracy & Technology*, Washington, DC. <https://doi.org/10.2139/ssrn.5348107>
- Gerke, S., Jacoby, M. B., & Cohen, I. G. (2025). Bankruptcy, genetic information, and privacy – Selling personal information. *New England Journal of Medicine*, 392(10), 937–939. <https://doi.org/10.1056/NEJMp2415835>
- Greely, H. T. (2020). The future of DTC genomics and the law. *Journal of Law, Medicine & Ethics*, 48(1), 151–160. <https://doi.org/10.1177/1073110520917003>
- Greenleaf, G. (2011). Global data privacy laws: Forty years of acceleration. *Privacy Laws and Business International Report*, (112), 11–17. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1946700](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1946700)
- Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying Personal Genomes by Surname Inference. *Science*, 339(6117), 321–324. <https://doi.org/10.1126/science.1229566>
- Hamilton, A. (2008, Oct. 29). Invention of the Year: 1. The Retail DNA Test. *Time Magazine*. [https://content.time.com/time/specials/packages/article/0,28804,1852747\\_1854493\\_1854113,00.html](https://content.time.com/time/specials/packages/article/0,28804,1852747_1854493_1854113,00.html)
- Hernandez, J. (2025, Mar. 24). 23andMe is filing for bankruptcy. Here's what it means for your genetic data. *NPR*, Washington, DC. <https://www.npr.org/2025/03/24/nx-s1-5338622/23andme-bankruptcy-genetic-data-privacy>
- Herper, M. (2025, Jun. 13). Anne Wojcicki wins back 23andMe, this time as a nonprofit. *STAT*, Boston, MA. <https://www.statnews.com/2025/06/13/23a>

- ndme-anne-wojcicki-wins-back-from-bankruptcy-will-become-nonprofit-ttam/
- Holpuch, A. (2013, Nov. 25). FDA orders genetics company 23andMe to cease marketing of screening service. *The Guardian*. <https://www.theguardian.com/science/2013/nov/25/genetics-23andme-fda-marketing-pgs-screening>
- Holthouse, R., Owens, S., & Bhunia, S. (2025). *The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies*. arXiv preprint. <https://doi.org/10.48550/arXiv.2502.04303>
- Kawaguchi, K., & Lee, M. H. (2025, Jun. 27). DNA For Sale: The Human Rights Crisis in the 23andMe Bankruptcy. *Health and Human Rights*. <https://www.hhrjournal.org/2025/06/27/dna-for-sale-the-human-rights-crisis-in-the-23andme-bankruptcy/>
- Kirk, R. (2025, Jun. 10). 23andMe Customers Did Not Expect Their DNA Data Would Be Sold, Lawsuit Claims. *New York Times*. <https://www.nytimes.com/2025/06/10/busines/23andme-data-lawsuit.html>
- Kotlan, A. M., Magoon, J. A., & Yates, D. J. (2026). Privacy Fragility in Direct-to-Consumer Genetic Testing: Lessons from the 23andMe Journey. *Hawaii International Conference on System Sciences (HICSS)*, Lahaina, Maui, HI.
- Kruchten, P., Nord, R. L., & Ozkaya, I. (2012). Technical debt: From metaphor to theory and practice. *IEEE Software*, 29(6), 18–21. <https://doi.org/10.1109/MS.2012.167>
- Lanzing, M. (2016). The Transparent Self: A Normative Investigation of Changing Selves and Relationships in the Age of the Quantified Self. *Philosophy & Technology*, 29(1), 33–48. <https://doi.org/10.1007/s10676-016-9396-y>
- Lee, J. B. (2025, Jul. 17). *23andMe Bankruptcy: The Privacy Ombudsman's Report*. Loeb & Loeb, New York, NY. <https://www.loeb.com/en/insights/publications/2025/07/23andme-bankruptcy-the-privacy-ombudsmans-report>
- McGuire, A. L., Caulfield, T., & Cho, M. K. (2008). Research ethics and the challenge of whole-genome sequencing. *Nature Reviews Genetics*, 9, 152–156. <https://doi.org/10.1038/nrg2302>
- Minsky, H. P. (1986). *Stabilizing an unstable economy*. Yale University Press.
- Narayan, S. M., Kohli, N., & Martin, M. M. (2025). Addressing contemporary threats in anonymized healthcare data using privacy engineering. *NPJ Digital Medicine*, 8, 145. <https://doi.org/10.1038/s41746-025-01520-6>
- Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61 Rev. 3)*. NIST, Washington, DC. <https://doi.org/10.6028/NIST.SP.800-61r3>
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–158. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>
- Phillips, A. M. (2016). Only a click away – DTC genetics for ancestry, health, love...and more: A view of the business and regulatory landscape. *Applied & Translational Genomics*, 8, 16–22. <https://doi.org/10.1016/j.atg.2016.01.001>
- Regalado, A. (2019, Feb. 11). More than 26 million people have taken an at-home ancestry test. *MIT Technology Review*. <https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/>
- Rutherford, A. (2025, Mar. 27). As a geneticist, I will not mourn 23andMe and its jumble of useless health information. *The Guardian*. <https://www.theguardian.com/commentisfree/2025/mar/27/geneticist-mourn-23andme-useless-health-information>
- Saey, T. H. (2025, Mar. 26). What 23andMe's bankruptcy means for your genetic data. *Science News*, Washington, DC. <https://www.sciencenews.org/article/23andme-bankruptcy-genetic-data-delete>
- Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYU Law Review*, 86, 1814–1894. <https://nyulawreview.org/issues/volume-86-number-6/the-pii-problem-privacy-and-a-new-concept-of-personally-identifiable-information/>
- Shabani, M., & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection

Regulation. *European Journal of Human Genetics*, 26(2), 149–156.  
<https://doi.org/10.1038/s41431-017-0045-7>

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, 141, 5–9.  
<https://doi.org/10.1016/j.ress.2015.03.018>

## APPENDIX A

### Sample Output of DNA Relatives Tool

Below are two important paragraphs about the DNA Relatives tool. These were taken directly (verbatim) from the 23andMe website in June 2025:

"The *DNA Relatives* feature is an interactive 23andMe feature, allowing you to find and connect with your genetic relatives and learn more about your family story. Genetic relatives (also known as DNA Relatives matches) are identified by comparing your DNA with the DNA of other 23andMe customers who are participating in the DNA Relatives feature. When two people are found to have an identical DNA segment, they very likely share a recent common ancestor. The DNA Relatives feature uses the length and number of these identical segments to predict the relationship between genetic relatives.

...  
To see your shared relatives, click on a match in your DNA Relatives list and scroll down to the *Relatives in Common* section. In this section, you can see the list of relatives that you have in common, the predicted relationship between each pair, and in some cases, if you share DNA in the same region of your genome. Keep in mind that only matches with whom you have a sharing connection or those showing ancestry results will display whether or not you share DNA in the same region of your genome."

You have 25 Relatives in Common™  
Finding common relatives can help you piece together your family story.

Relative in common	You	Relative	Shared DNA
<b>EU</b> Example Uncle	Uncle (24.0%)	4th Cousin (0.29%)	Yes
<b>ER</b> Example Relative	4th Cousin (0.39%)	5th Cousin (0.12%)	No
<b>ER</b> Example Relative	4th Cousin (0.34%)	5th Cousin (0.18%)	No
<b>ER</b> Example Relative	4th Cousin (0.29%)	4th Cousin (0.28%)	Share to see

**Figure 1: Sample Output from DNA Relatives Tool**  
(Source: <https://customercare.23andme.com/hc/en-us/articles/221689668-DNA-Relatives-In-Common-Report-Feature>)

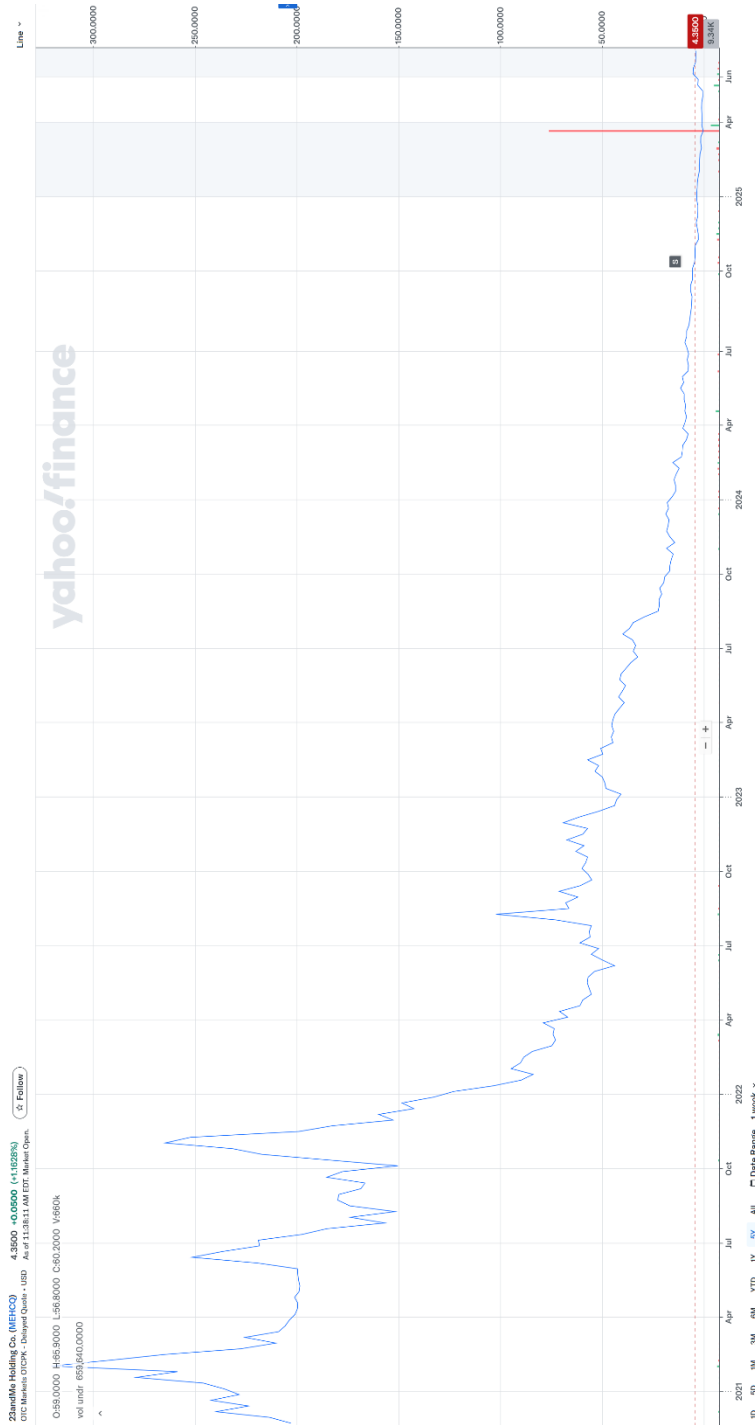
As of September 2025, this tool includes the following disclosure:

"We have temporarily disabled some features within the DNA Relatives tool as an additional precaution to protect your privacy. Read more [here](#)."

## APPENDIX B

### Timeline of 23andMe Milestones

#### 23andMe Share Price Versus Time



## 23andMe Timeline (2006 – September 2025)

- **2006** – 23andMe is founded by Anne Wojcicki, Linda Avey, and Paul Cusenza with the aim of democratizing access to genetic testing for health and ancestry (McGuire, Caulfield & Cho, 2008).
- **2008** – The company gains major public attention; its testing kit is named Time magazine's *Invention of the Year* (Hamilton, 2008).
- **2013** – The U.S. FDA orders 23andMe to halt health-related genetic reporting, citing concerns over unvalidated medical risk interpretations (Holpuch, 2013). The company temporarily suspends parts of its product.
- **2015–2018** – 23andMe relaunches health reports and enters into a \$300 million partnership with GlaxoSmithKline (GSK) to leverage aggregated genetic data for drug discovery (23andMe, 2018). By February 2018, there are ~3 million customers.
- **2018** – 23andMe solidifies its position as a leader in the direct-to-consumer genetics market (Regalado, 2019).
- **June 2021** – The company goes public via SPAC at ~\$3.5B valuation; ~12M customers at close (23andMe, 2021).
- **2022** – 23andMe faces increased scrutiny over privacy practices and monetization strategies. Growth slows even though the company surpasses 12 million genotyped customers (23andMe, 2022).
- **May 2023** – The company reported >14 million genotyped customers (Holthouse, Owens & Bhunia, 2025); lawmakers later referred to more than 15 million during 2025 oversight and bankruptcy proceedings. <https://oversight.house.gov/release/wrap-up-congress-taking-action-to-ensure-the-safety-of-americans-personal-dna-data/>
- **October 2023** – 23andMe suffers a credential-stuffing attack affecting ~14,000 accounts and indirectly exposing profile data from 6.9 million users through the DNA Relatives feature. The company does not issue full disclosures until months later (23andMe, 2024; Hernandez, 2025).
- **January 2024** – California AG breach notice filed (23andMe, 2024). Reported ~14,000 accounts accessed via credential-stuffing; noted forced password resets and MFA expansion.
- **Late 2024** – Trust in the platform declines, and user engagement drops. Still, estimates suggest ~15 million cumulative users remain in the database (Hernandez, 2025).
- **October 2024** – 23andMe executed a 1-for-20 reverse stock split to raise its share price above the NASDAQ minimum listing requirement after its stock had fallen below \$1 for an extended period. <https://www.nasdaqtrader.com/TraderNews.aspx?id=ECA2024-495>
- **March 2025** – The company files for Chapter 11 bankruptcy, citing falling revenue, reputational damage, and unresolved legal claims. CEO Anne Wojcicki steps down from leadership (Hernandez, 2025; Herper, 2025).
- **June 2025** – 23andMe had accumulated class-action lawsuits and faced regulatory action in the U.S., U.K., and Canada. The UK ICO fined the company £2.31 million following a joint investigation with Canada's OPC (Kawaguchi & Lee, 2025; Kirk, 2025).
- **July 2025** – Wojcicki's new non-profit venture, TTAM Research Institute, successfully purchases 23andMe's assets – including its genetic data – for \$305 million in a bankruptcy auction, outbidding firms like Regeneron. This sale raises unprecedented concerns over data transfer ethics, user consent, and platform accountability in the DTC-GT industry (Herper, 2025; Kawaguchi & Lee, 2025).
- **September 2025** – 23andMe seeks approval for a \$50 million class-action settlement; this reflects an increase from the \$30 million preliminarily approved in December 2024. <https://www.reuters.com/legal/government/23andme-seeks-approval-larger-50-million-data-breach-settlement-2025-09-05/>

## APPENDIX C

### Technical Vulnerabilities and Security Failures that Contributed to the 23andMe Breach

Category	Failure or Weakness	Implication
<b>Authentication</b>	No mandatory multi-factor authentication (MFA)	Allowed attackers to access accounts using stolen passwords alone
<b>Access Control</b>	Inadequate rate limiting and anomaly detection on DNA Relatives queries	Enabled lateral exposure of millions of profiles from a small number of compromised accounts
<b>Credential Management</b>	Susceptible to credential stuffing due to weak password reuse protection	Exploited passwords reused across platforms; lacked protections against bulk login attempts
<b>Logging and Monitoring</b>	Insufficient real-time monitoring of unusual query behavior	Delayed detection and containment of attacker activity
<b>Data Minimization</b>	Broad data exposure via the DNA Relatives feature	Enabled visibility of names, ancestry, and relationships beyond the originally compromised account
<b>Incident Response</b>	Absence of a formal incident response plan aligned with NIST SP 800-61 Rev. 3	Delayed disclosure and inconsistent regulatory communication
<b>User Consent Architecture</b>	No granular or retroactive consent options for shared data	Users had no ability to limit relational data exposure post-breach
<b>Third-Party / Data Governance</b>	Lack of vendor risk assessment and unclear data-sharing boundaries during research partnerships	Elevated risk of secondary exposure and uncertainty during bankruptcy or data transfer