

## 23andMe Bankruptcy Sparks Data Privacy Concerns. Should It?

### Hashed & Salted | A Privacy and Data Security Update

In the legal industry, handling business transactions is part of our daily routine. Managing the transfer of personal data during acquisitions, sales, mergers or bankruptcy proceedings has become second nature to us. We perform thorough due diligence for these deals, ensure that privacy policies allow for the transfer of personal data, and negotiate the necessary contracts with current partners and data recipients—crucial steps that can enhance the business’s valuation.

Against this backdrop, the current discourse surrounding the 23andMe bankruptcy filing raises questions. Regulators and consumer privacy advocates are urging individuals to delete the data 23andMe holds on them, and are [advocating](#) for stronger privacy legislation. The court-appointed Consumer Privacy Ombudsman (CPO) in the case issued a report June 11 raising concerns about the sale of information in connection with bankruptcy. (For more on the CPO’s Report, read our article [“23andMe Bankruptcy: The Privacy Ombudsman’s Report.”](#))

Many of these concerns stem from the uncertainty regarding the potential acquirer, their possible intentions for using the genetic and lineage data, and the lack of sufficient legal protections for consumers. This reaction seems disproportionate, however. Similar alarms are not raised for every business transaction involving personal data, and even the 2023 security breach at 23andMe didn’t trigger this level of concern. So, why would a bankruptcy sale warrant such alarm?

Data breaches, particularly involving sensitive information, pose significant risks. Bad actors often evade justice, making it easier for stolen data to circulate among



other malicious entities. For them, the rule of law is irrelevant—the value lies in gaining access to and the use of a treasure trove of personal data for their own gain. In contrast, any acquirer of 23andMe would face stricter scrutiny and legal obligations, including compliance with privacy policies, robust security measures and existing laws governing such transactions. Any acquirer would be obligated to uphold the commitments 23andMe made to its customers during onboarding. Therefore, the call for individual data deletion by 23andMe customers would be both unnecessary and detrimental to the sale of the business to a legitimate buyer.

Arguments that the fragmented nature of state privacy laws, specialized health/genetic data laws and HIPAA creates too many gaps in consumer protection are off target. In the context of the transfer of personal data between businesses, existing legal obligations—enforceable at federal, state and local levels under consumer protection laws such as unfair, deceptive or abusive practices (UDAP) statutes—provide a foundation for safeguarding data during business transactions. If adhered to and enforced, these legal principles ensure such transactions are not inherently harmful to consumers.

*Attorney Advertising*

Personal data is frequently portrayed as the cornerstone of business value in the transaction. However, personal data's worth is directly tied to the strength of the target company's privacy and security practices. Companies that prioritize transparency, obtain consent and invest in data protection are inherently more valuable. Conversely, weaker data protection practices diminish business value. Extensive due diligence during negotiations assesses these practices and informs the terms of business transfer agreements, which typically include representations and warranties regarding compliance with applicable laws. Both parties—the target and the acquirer—commit to upholding legal standards.

To transfer personal data as part of a transaction, the transfer must be explicitly disclosed in the privacy policy at the time of data collection. Without such disclosure, notice and consent are required—even if the privacy policy allows updates at any time. Retroactive changes to processing practices without notice and consent violate UDAP statutes. Tools like the Wayback Machine ensure accountability by preserving snapshots of privacy policies.

Similarly, any acquirer of 23andMe must adhere to the existing privacy policy and is prohibited from materially altering the usage of the data without notice and consent. Any new purposes, security measures or disclosure practices require explicit consumer approval. As 23andMe is recognized for its [stringent privacy protections](#), an acquirer must maintain these standards. Additionally, the acquirer is bound by the heightened security measures from the \$30 million settlement following the 2023 breach, which affected approximately 14,000 accounts via credential stuffing.

If regulators and consumer privacy advocates trust 23andMe's current practices, there is little reason to doubt those of the acquirer, provided they comply with the same obligations. For instance, if 23andMe does not share genetic data for hiring, insurance or other purposes without consent, neither can the acquirer. Even sharing data with law enforcement outside valid legal requests would require consent. Consumer rights, including the ability to delete their data, must also be maintained.

The FTC and state attorneys general consistently enforce UDAP statutes concerning data transfers in business transactions. While stronger privacy laws may be beneficial, a deeper understanding and enforcement of existing legal obligations are critical. These measures foster trust among regulators, businesses and consumers while preserving the value of companies undergoing acquisitions.

---

### Related Professionals

Allison Cohen . . . . . ahcohen@loeb.com  
Teodoro "Teddy" Shelby . . . . . tshelby@loeb.com

---

*This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.*

© 2025 Loeb & Loeb LLP. All rights reserved. 8005 REV1 080625