.

TESTIMONY AND STATEMENT FOR THE RECORD

Margaret Hu
Davison M. Douglas Professor of Law
Director, Digital Democracy Lab
William & Mary Law School

"Securing Americans' Genetic Information: Privacy and National Security Concerns Surrounding 23andMe's Bankruptcy Sale."

House Committee on Oversight and Government Reform
U.S. House of Representatives

June 10, 2024

Good Morning, Chairman Comer and Committee Members:

I am Margaret Hu, Davison M. Douglas Professor of Law and Director of the Digital Democracy Lab, at William & Mary Law School in Williamsburg, Virginia. Thank you for the opportunity to address the urgent matter of how best to secure Americans' genetic data privacy. As this Committee recognizes, the collection, storage, and analyses of sensitive genetic information and, and its disclosure, can pose a range of national security concerns and risks. The bankruptcy proceedings of 23andMe demonstrates why these matters are so consequential, especially in the Age of Artificial Intelligence (AI) and the future of AI warfare.

The first decade of my law career was dedicated to the Civil Rights Division of the U.S. Department of Justice. My first day as a Trial Attorney in the U.S. Department of Justice was the day before the terrorist attack of September 11, 2001. I immediately joined a post-9/11 Task Force and focused on homeland security and border security policy matters.

In the past decade, I have served as a researcher and professor of AI Law, Constitutional Law, and National Security Law. I would like to approach this topic from the perspective of AI and National Security Law. My post-9/11 policy work introduced me to the topics that now form the basis of my current research in data privacy, cybersecurity, and AI governance, with a particular focus on biometric cybersurveillance

and biometric cyberintelligence.

This hearing is critically important. Genetic data and biometric cyberintelligence lies at the very center of a new battlefield in the Age of AI. Safeguarding the genetic data of 23andMe and other biotech corporations is not just a matter of data privacy. It is of paramount importance as a matter of national security. Consequently, in addition to discussing the bankruptcy and consumer data protection laws of this current matter, I am grateful for the opportunity to support this Committee's examination of the national security implications of the sale and transfer of 23andMe data and 23andMe bankruptcy proceedings.

Background

The topic of genetic data privacy, unfolding within the context of the bankruptcy proceedings of 23andMe is simultaneously unfolding within the context of a larger crisis: inadequate federal data privacy and cybersecurity safeguards generally, and inadequate federal laws to address the challenges of the AI revolution. The 23andMe bankruptcy filing is a wakeup call that our current legal inadequacy amounts to instability in our national security.

In the Age of AI, data privacy, cybersecurity, and AI infrastructure form a tapestry of overlapping systems of technology and law. The Federal Aviation Administration (FAA), for example, coordinates airspace and air traffic control; aircraft safety and investigation; and sets standards for the national airport systems. Without question, the FAA is seen as an essential national security partner, coordinating closely with the U.S. Department of Defense, as it supports both civil and military aircrafts.

The 23andMe bankruptcy matter provides a window into why Congress should step forward to enact laws that are capable of creating a similar administrative oversight structure, including regulations that acknowledge the need to coordinate national security concerns in the handling of sensitive genetic data such as the datasets held by 23andMe and other commercial genetic testing companies.

Congress should act immediately to enact both federal data privacy laws and cybersecurity laws. Next, Congress can take legislative action to enact a federal AI law that anticipates the significant national security threats that can be posed by inadequate AI regulations.

23andMe holds the genetic and personal data of over 15 million individuals, including predispositions to disease, ancestral background, and familial linkages. This data is not only personal and permanent, it is relational: disclosing one person's genetic information may affect entire family trees, making the stakes unusually high.

Almost 7 million consumers were exposed in a data breach of 23andme in 2023.[1] The company entered into a settlement agreement that involved a $30 million settlement and a promise of three years' worth of security monitoring.[2] In March 2025, 23andMe filed for Chapter 11 bankruptcy protection. Its most valuable asset is its genetic database, now the subject of a bidding process. A $256 million bid from Regeneron Pharmaceuticals was followed by a $305 million counter-offer from Anne Wojcicki, the company's co-founder, through her nonprofit TTAM Research Institute.

Bankruptcy law allows the appointment of a Consumer Privacy Ombudsman under certain conditions under 11 U.S.C. § 363(b)(1)(B). Yet, the ombudsman's role is advisory, not determinative. In the case of the 23andMe bankruptcy matter, Professor Neil Richards, Koch Distinguished Professor in Law at Washington University in St. Louis—an expert in privacy law—was appointed as the ombudsman by U.S. Bankruptcy Judge Brian Walsh.

23andMe's original privacy policy represented to users that their data would not be shared without consent. However, it is now in the hands of bankruptcy law to assess whether these original promises can be reneged and whether the incoming buyer of 23andMe will override these original expectations. Without a federal genetic privacy framework and an omnibus federal data privacy law, this data could be sold—even to entities with entirely different purposes.

The federal government does not provide data privacy or data protection guidance for DNA kit companies like 23andMe. There is no specific minimum cybersecurity safeguards required under federal law either. Very general consumer protection laws, for example, are not adequate here, especially since

[1] Kevin Williams, *23andMe bankruptcy: With America's DNA put on sale, market panic gets a new twist*, CNBC (updated Mar. 30, 2025), https://www.cnbc.com/2025/03/30/23andme-bankruptcy-selling-deleting-dna-genetic-testing.html.
[2] *Id*.

we're talking about highly sensitive genetic information that is linked to highly sensitive consumer profile information, such as ethnicity and race, birth date, and other data.

The company's cybersecurity system might be even more exposed now that they are facing financial duress. When the sale of a company is imminent, there is the potential that cybersecurity and data protection protocols are necessarily prioritized. Also, many employees flee when a company declares bankruptcy. Employees who were charged with enforcement of data privacy agreements of the company or tasked with safeguarding the data may be departing soon, either by securing another employment opportunities at other companies or through layoffs, or through reorganization, once the sale of 23andMe is completed.

This creates a very unstable environment for protecting extremely sensitive data. Media reports state that the company has already terminated over 40% of its employees. Who is left to safeguard this data? In a time of financial vulnerability, companies such as pharmaceutical companies might see an opportunity to exploit the research benefits of the genetic data. They might try to renegotiate prior contracts to extract more data from the company. Currently, 23andMe states that when it sells genetic data to other research companies, it strips away identifying data from the genetic data. Will they continue to do that? Will the next company that buys 23andMe honor those same commitments?

23andMe states that it is committed to indentifying a buyer who shares its privacy values. Yet, the concern remains that the new owner of 23andMe might repurpose or share the genetic data in ways that the consumer did not intend. The new owner of the genetic data currently held by 23andMe might sell it off, piece by piece, indiscriminately. And the buyer of that data might be a foreign adversary. There is a black market for sensitive genetic data and foreign adversaries are fighting to get this data as well for a wide range of reasons, including for strategic advantage, sometimes referred to as military identity dominance, or biometric cybersurveillance or biometric cyberintelligence.

Biometrics and National Security

Biometrics is defined as "[t]he science of automatic identification or identity verification of

individuals using physiological or behavioral characteristics."[3] Perceived as both unique and immutable, in the context of border security and national security, biometric data is often construed as a type of "gold standard" for identity assessment and verification.[4] Biometric data can include both hard and soft biometrics,[5] often distinguished by the "perceived reliability for automated identification matching technologies."[6] Traditionally, hard biometrics have included the types of biometric data points that are now categorized and captured by the U.S. Department of Homeland Security (DHS), including facial recognition technology, iris scans, digital fingerprints and palmprints, and DNA.[7] In contrast to hard biometrics, "soft biometrics" are often understood to include age, height, weight, race or ethnicity, skin and hair color, scars, birthmarks, tattoos, and other physiological characteristics that, although considered less stable than hard biometrics, can still be subject to digital capture, and automated identification and assessment protocols.[8] Soft biometrics are defined as "anatomical or behavioral characteristic[s] that provide[] some information about the identity of a person, but does not provide sufficient evidence to precisely determine the identity."[9] Both DHS and the U.S. Department of Defense (DoD) rely upon the collection and analysis of both hard and soft biometrics in multiple contexts.[10]

---

[3] JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007).
[4] Alan Gomez, Immigrant Tracking May Impede Bill; Partisan Split Developing over Biometric Data on Foreigners Leaving U.S., USA TODAY, May 9, 2013, at A5 ("[Former U.S. Secretary of Homeland Security Michael] Chertoff calls [biometrics] the 'gold standard.'").
[5] Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 661 n.287 (2017); Margaret Hu, Biometric Surveillance and Big Data Governance in CAMBRIDGE HANDBOOK ON SURVEILLANCE LAW 125–26 (David Gray and Stephen Henderson, eds.) (2017).
[6] *Id*.
[7] DEPT. HOMELAND SEC., BIOMETRIC TECHNOLOGY REPORT: EO 14074, 13(E) (Dec. 2024), https://www.dhs.gov/publication/biometric-technology-report.
[8] *Id*.
[9] *See* Karthik Nandakumar & Anil K. Jain, *Soft Biometrics, in* ENCYCLOPEDIA OF BIOMETRICS 1235, 1235 (Stan Z. Li & Anil Kumar Jain eds., 2009).
[10] *See, e.g.*, Dept. Defense, *Contracts For June 17, 2024, Navy* ("Small Business Innovation Research Phase III topic N08-077 titled 'Automated Entity Classification in Video Using Soft Biometrics'"), https://www.defense.gov/News/Contracts/Contract/Article/3809606/; DEPT. HOMELAND SEC., BIOMETRIC SYSTEMS APPLICATION NOTE (June 2015), https://www.dhs.gov/sites/default/files/publications/Biometric-Sys-AppN_0615-508.pdf.

Biometric cybersurveillance and cyberintelligence underscore the perceived value of biometric data collection for military and intelligence purposes.[11] Within national security, "biometrically enabled intelligence,"[12] or "biometric-enabled intelligence,"[13] means the establishment of "an analytical baseline by resolving identities through high-confidence biometric matching and fusion with other sources of intelligence to positively identify the person in question."[14] In the intelligence and military use context, biometric cybersurveillance and cyberintelligence can make identities of potential criminals and terrorists more fully transparent. Amassing "multiple biometric data points and other biographic data purportedly enhances the ability of the government to identify potential enemies of the state through mass data collection and analysis."[15]

To better understand the story of why genetic data and the fusion of biometric and biographic data are anchoring a new chapter in how modern nation states wage war, it is important to consult sources such as Annie Jacobsen's book, *First Platoon: A Story of Modern War in the Age of Identity Dominance*,[16] the Snowden disclosures, and other surveillance revelations of the past two decades. A 2010 NSA document revealed in the *New York Times* as part of the Snowden disclosures explained: "'It's not just the traditional communications we're after: It's taking a full-arsenal approach that digitally exploits the clues a target leaves behind in their regular activities on the net to compile biographic and biometric information' that can help 'implement precision targeting[.]'" Media reports increasingly describe AI-driven targeting

---

[11] Margaret Hu, *Biometric Cyberintelligence and the Posse Comitatus Act*, 66 EMORY L. J. 697, 701-703 (2017) (citations omitted).
[12] *Id.* at 703 n.24 (citing Ben Iannotta, *Biometrics: A New Intelligence Battlefield; Brings Tech Choices & Challenges*, FORTUNA'S CORNER (May 14, 2013), http://fortunascorner.com/2013/05/14/biometrics-a-new-intelligencebattlefield-brings-tech-choices-challenges).
[13] *Id.* at 703 n.25 (citing David Pendall & Cal Sieg, *Biometric-Enabled Intelligence in Regional Command-East*, 72 JOINT FORCE Q., 1st Quarter 2014, at 69, 70, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72_69-74_PendallSieg.pdf?ver=2014-03-13-152414-890).
[14] *Id.* at 703 n.26 (citing Paul Moruza, *Intelligence Center Develops Biometrically Enabled Intelligence to Support Warfighter*, U.S. ARMY (Jan. 8, 2013), http://www.army.mil/article/93969/Intelligence_center_develops_Biometrically_Enabled_Intelligence_to_support_warfighter/ (quoting Cathy Moore, Senior Intelligence Analyst, U.S. Army, Biometrics Division, National Ground Intelligence Center)).
[15] *Id*.
[16] ANNIE JACOBSEN, FIRST PLATOON: A STORY OF MODERN WAR IN THE AGE OF IDENTITY DOMINANCE (2021).

decisions[17] that may be informed by biometric-biographic profiling and data-driven assessments of threat.

Genetic Data and National Security Risks

The national security risks of misuses and abuses of the genetic data by foreign adversaries include biological warfare risks, blackmail, and increased surveillance, among other potential threats. The Pentagon had previously warned military personnel that DNA kits could pose a risk to national security.[18] Specifically, in 2019, then-Under Secretary of Defense for Intelligence, Joseph D. Kernan noted that consumer genetic testing products can "pose[] personal and operational risks to Service members."[19] The U.S. Department of Defense warned that "outside parties are exploiting the use of genetic data for questionable purposes, including mass surveillance and the ability to track individuals without their authorization or awareness."[20] Other harms include abusing genetic data for isolating and discriminatory targeting,[21] and potentially analyzing genetic data and aggregating biometric data with biographical data for the purposes of cognitive warfare.[22] After the 23andMe breach of in 2023, the class action lawsuit that followed alleged that customers of specific ethnic heritages were targeted, with genetic information shared on curated lists published on the dark web.[23]

Other national security concerns stem from the sale of 23andMe and its genetic databases. There is currently no bar on foreign investment in consumer genetic testing companies. Although there is no ITAR

---

[17] *See generally*, Marten Zwanenburg, *Biometrics on the Battlefield*, Lieber Institute, West Point (Oct. 21, 2020); Jimena Sofia Viveros Alvarez, *The Risks and Inefficacies of AI Systems in Military Targeting Support*, Int'l Committee of the Red Cross (Sept. 4, 2024).

[18] Memorandum from Joseph D. Kernan, Under Secretary of Defense for Intelligence and James N. Stewart, Assistant Secretary of Defense for Manpower and Reserve Affairs, Performing the Duties of the Under Secretary of Defense for Personnel and Readiness, Direct-to-Consumer Genetic Testing Advisory for Military Members (Dec. 20, 2019), https://www.scribd.com/document/440727436/DOD-memo-on-DNA-testing.

[19] *Id.*

[20] *Id.*

[21] *See, e.g.*, Rebecca Carballo, Emily Schmall, and Remy Tumin, *23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says* (Jan. 26, 2024); Julian E. Barnes, *U.S. Warns of Efforts by China to Collect Genetic Data*, N.Y. Times (Oct. 22, 2021).

[22] Sara Rajtmajer and Daniel Susser, *Automated Influence and the Challenge of Cognitive Security,* In Proceedings of the 7th Symposium on Hot Topics in the Science of Security, HotSoS 2020 (pp. 62-70). (ACM International Conference Proceeding Series). Association for Computing Machinery. https://doi.org/10.1145/3384217.3385615; Łukasz Kamieński, *Beyond Defense: A Call to Arms for Cognitive Warfare*, Center for Ethics and the Rule of Law, University of Pennsylvania (May 9, 2024)**.**

[23] *See* Carballo, et al., *supra* note 19.

(International Traffic in Arms Regulations) equivalent to protecting genetic data, Congress has now passed the Protecting Americans' Data from Foreign Adversaries Act, which demonstrates growing awareness of the need to protect sensitive data for national security purposes.

Conclusion

The federal government must enact strong data protection laws. The California Attorney General's Office urged California residents to ask the company to delete their data from 23andMe and to ensure that California citizens opted out of any future data for research or genetic data storage.[24] But this is the guidance that should have been provided to all U.S. citizens, not just California residents. Federal data privacy laws demand parallel enactment of federal cybersecurity laws and AI regulations as well. Data privacy is not only a consumer data privacy issue, but also a national security one. In light of the significant national security risks that attach to sensitive personal data, should Americans' most sensitive health and hereditary information be sold as a corporate asset without meaningful consent or adequate legal protection? The answer must be no.

[24] Press Release, Rob Bonta, California Attorney General, Attorney General Bonta Urgently Issues Consumer Alert for 23andMe Customers (March 21, 2025), https://oag.ca.gov/news/press-releases/attorney-general-bonta-urgently-issues-consumer-alert-23andme-customers.