S. HRG. 119–200

23 AND YOU: THE PRIVACY AND NATIONAL SECURITY IMPLICATIONS OF THE 23ANDME BANKRUPTCY

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JUNE 11, 2025

Serial No. J–119–22

Printed for the use of the Committee on the Judiciary

www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–889 WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

LINDSEY O. GRAHAM, South Carolina	RICHARD J. DURBIN, Illinois, *Ranking Member*
JOHN CORNYN, Texas	SHELDON WHITEHOUSE, Rhode Island
MICHAEL S. LEE, Utah	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	CHRISTOPHER A. COONS, Delaware
JOSH HAWLEY, Missouri	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	MAZIE K. HIRONO, Hawaii
JOHN KENNEDY, Louisiana	CORY A. BOOKER, New Jersey
MARSHA BLACKBURN, Tennessee	ALEX PADILLA, California
ERIC SCHMITT, Missouri	PETER WELCH, Vermont
KATIE BOYD BRITT, Alabama	ADAM B. SCHIFF, California
ASHLEY MOODY, Florida	

KOLAN DAVIS, *Chief Counsel and Staff Director*
JOE ZOGBY, *Democratic Chief Counsel and Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

23 AND YOU: THE PRIVACY AND NATIONAL SECURITY IMPLICATIONS OF THE 23ANDME BANKRUPTCY

WEDNESDAY, JUNE 11, 2025

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:19 a.m., in Room 226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley [presiding], Cornyn, Hawley, Blackburn, Britt, Moody, Durbin, Klobuchar, Coons, Padilla, and Schiff.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman GRASSLEY. Good morning, everybody.

Genetic data is the blueprint to a person. It is sensitive, it is personal, and in the wrong hands, it can be dangerous. As technology and biotechnology rapidly expand, they bring new and serious challenges. Consumers deserve to know how their data is going to be used, and Americans deserve protection from foreign threats. That is why we are here today.

The 23andMe saga has unveiled serious and concerning issues regarding consumer protection, data privacy, and national security. We have explored these issues in these hearings, but today's hearing focuses upon genetic data. 23andMe collected genetic data from roughly 15 million people, and when it did, it told the consumers that their data would be safe. They said it would be protected under their privacy policy.

But now, 23andMe is in bankruptcy, and it is selling off its data, Americans' genetic data, your data, to the highest bidders, bidders who consumers never consented to giving their information to, bidders who could manipulate and repurpose the genetic data, bidders who could be loyal to or controlled by foreign adversaries. Without any Federal law governing genomic data privacy, the only protection for the American consumer was 23andMe's own privacy policies.

Even putting aside whether consumers read or understood the privacy policy, they were required to sign it as-is, or they couldn't use the service. And now that 23andMe is in bankruptcy, whichever company buys them can change the privacy policy on a whim, however they see it.

That's why, just yesterday, 27 States sued to block the sale of this data. Though the bankruptcy code requires a consumer privacy ombudsman to be appointed when personally identifiable data is being sold in violation of a privacy policy, that simply is not enough. On the one hand, the bankruptcy code doesn't include genetic data within the definition of these three words, personally identifiable information. So even if a company sold genetic data in violation of their privacy policy, the code doesn't require an ombudsman to be appointed to protect consumer privacy interest.

On the other hand, even if an ombudsman is appointed, the timeline for on which they operate and the efficacy of their role must be further interrogated. Before Americans' genetic information is sold, they should be able to decide whether, when, and how that data is going to be used.

In addition to consumer rights concerns, the national security implications of 23andMe bankruptcy are significant. In 2019, the Department of Defense issued guidance that servicemembers refrain from using direct-to-consumer DNA testing kits. When a consumer genetics company accumulates the personal genomic blueprint of millions, many of whom are U.S. citizens, government employees, or military personnel, it becomes a strategic intelligence asset. In the wrong hands, this data access isn't just a privacy breach, it is a potential weapon.

Foreign governments can design targeted biological weapons and wage pathogenic warfare. They can identify health vulnerabilities and conduct tailored attacks on key military and government personnel. In light of the serious evidence that COVID–19 was created in a Chinese laboratory, the weaponization of biologics and the military application of genomic data are no longer far-fetched fantasies of science fiction. They are tenable threats to the national security.

The threat from China is particularly acute. The Chinese have invested heavily in their military-civil fusion strategy where they seek to erase the line between private property and military assets. The Chinese Communist Party aggressively integrates development of artificial intelligence, biotech, and computing into their military efforts. They seize and acquire corporate assets to engage in unconventional and asymmetric warfare.

Just this week, for example, two Chinese nationals were charged with smuggling a dangerous pathogen used for agricultural terrorism into the United States. The Chinese Government paid for one of the nationals to research this pathogen, and a search of their electronics revealed information linking them to the Chinese Communist Party.

Data is a weapon, and genetic data is particularly a potent weapon. Americans' genetic data must be zealously defended and jealously protected. The 23andMe bankruptcy is a massive threat to the protection of the genetic data of so many Americans.

Congress has yet to enact sufficient protection on these important issues. There is no data privacy law that protects genomic data, no provision in the bankruptcy code that prevents this data from being compromised through bankruptcy auction, and no sufficient remedy for consumers.

I recently co-sponsored Senator Cornyn's Don't Sell My DNA Act, which aims at filling some of these gaps, but there is a lot more work to do. I look forward to hearing from our witnesses about how we can advance legislation that better protects Americans' genetic security.

With that, I will open things up to Senator Durbin to give an opening statement. Then, we will hear from our witnesses.

OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Senator DURBIN. Thanks, Senator Grassley, good and timely hearing as far as I am concerned.

23andMe has a data base containing the genetic information of about 15 million people. If your genetic information is in their data base, a researcher can tell you who your relatives are, what your ethnicity is, what your eye color is, and whether you think cilantro tastes like soap. They can also determine a lot of information about your health. Are you at risk of developing type 2 diabetes? How about celiac disease, chronic kidney disease, Parkinson's?

In short, 23andMe has access to deeply personal information about you and your health, information that you would normally want to keep private, I guess, between you and your family and your doctor. Yet no federal law, no federal law, prevents 23andMe from sharing this data with others, including insurance companies, future employers, and law enforcement. Rather, a patchwork of State laws, privacy policies are the only things protecting the genetic information of millions of Americans.

If 23andMe's customers are anything like fellow Americans, they likely did not read this privacy policy. According to a survey by Pew Research, more than half Americans say they always—well, almost always—often agree with privacy policies without ever reading them. Who can blame them? Whether you are activating your cell phone, setting up your Facebook account, accessing a number of services, Americans are bombarded with countless privacy policies to which they must agree, and virtually all of us do.

One company who studied the issue found that Americans would have to spend, get ready, 47 hours a month to read the privacy policies of the most visited websites. That is more than a full 9 to 5 workweek every single month. Get real.

When 23andMe filed for bankruptcy on March 23, a lot of people suddenly became interested in privacy policy because buried in the fine print of their privacy policy is the following. Listen closely. "If we are involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your personal information may be accessed, sold, or transferred as part of the transaction." Remember that clause? Probably not.

So 23andMe's 15 million customers are left wondering, who is going to get access to my genetic information? What are they going to do with it? What rights do I have to stop it? That is why we need this hearing.

Thankfully, 23andMe's privacy policy gave its customers the right to delete their data upon request, and millions have done so, so many, in fact, that 23andMe's website crashed with the traffic. Again, this wasn't required by Federal law. There are very few fed-

eral guardrails to protect the most sensitive personal data, including your DNA and who can share it.

It is time for Congress to put some protections in place for Americans. In the right hands, a genetic data base could help researchers unlock lifesaving medical cures and make incredible discoveries. But in the wrong hands, in the wrong hands, it could enable dystopian discrimination, and surveillance could be used by our adversaries. You were turned down for that job? Why did they turn me down? Turns out they knew a lot more about you than you knew about yourself.

The American people deserve to have faith that their sensitive information will be and stay in the right hands before they agree to share it. Yet nearly 20 years after 23andMe came on the scene, and at least that long since the surveillance industrial complex started taking over the internet, America still lacks a comprehensive federal law to protect our privacy. Like other areas, including kids' online safety, to which this Committee has dedicated a lot of time, there is bipartisan consensus that something needs to be done about our privacy.

There have been signs of hope, including in 2022 when the American Data Privacy and Protection Act passed the House by a broad bipartisan vote of 53 to 2. This is the Energy and Commerce Committee. But the American people are still waiting. I think we can get together and pass a bipartisan bill. This hearing might help.

Thanks, Mr. Chairman.

Chairman GRASSLEY. Thank you.

This is a consensus hearing, so I am going to go ahead and introduce all the witnesses that have joined us today. Then, I will swear them in.

Mr. Joseph Selsavage serves as interim CEO, CFO, CAO, 23andMe, joined 23andMe in November 2021 through the acquisition of Lemonaid Health. At Lemonaid Health, he was chief financial officer. Mr. Selsavage received a BA in economics and financial management and his MA in accountancy from Catholic University. He also received his MBA from Massachusetts Institute of Technology. He is a certified public accountant.

Next, we have Mr. Glenn Cohen, professor of law at Harvard Law School and the faculty director of Harvard Center of Health Law Policy, Biotechnology, and Bioethics. Professor Cohen is an elected member of the National Academy of Medicine and has spoken to NATO, OECD, and members of the U.S. and Korean Congress on medical and biotech issues and policies. He previously served as a lawyer for the U.S. Department of Justice, Civil Division, where he handled litigation in Court of appeals and U.S. Supreme Court.

Next, we have Ms. Brook Gotberg, professor of law, Brigham Young University. Professor Gotberg teaches bankruptcy, contracts, secured transactions, and other commercial law subjects. Her scholarship focuses on debtor and creditor relations and various impacts on the bankruptcy code and business reorganization. Professor Gotberg earned her BA in political science magna cum laude, Brigham Young University, and her JD cum laude from Harvard Law School.

Mr. Adam Klein is a senior lecturer at UT Austin School of Law and director of the Strauss Center for International Security and Law. Previously, Mr. Klein served as chairman and CEO of the United States Privacy and Civil Liberties Oversight Board, overseeing counterterrorism programs at the NSA, FBI, CIA, and the Department of Homeland Security. Before entering government, Mr. Klein was a senior fellow at the Center for the New American Security and National Security Think Tank. Earlier in his career, he served as a law clerk to Justice Scalia of the Supreme Court.

Would you please rise so I could administer the oath?

[Witnesses are sworn in.]

Chairman GRASSLEY. Thank you. And I think we will go my left to my right, so you start, Mr. Selsavage.

STATEMENT OF JOSEPH SELSAVAGE, INTERIM CHIEF EXECUTIVE OFFICER AND CHIEF FINANCIAL AND ACCOUNTING OFFICER, 23ANDME HOLDING CO., SOUTH SAN FRANCISCO, CALIFORNIA

Mr. SELSAVAGE. Chairman Grassley, Ranking Member Durbin, and Members of the Committee, thank you for the opportunity to appear before you today. My name is Joseph Selsavage, and I am the interim chief executive officer of 23andMe, a mission-driven organization founded on the simple yet transformative belief that individuals have the right to access, understand, and benefit from their own genetic information. From the very beginning, 23andMe's purpose has been clear, to help people live healthier lives through direct access to their own DNA, to accelerate scientific discovery, and to contribute meaningfully to the future of personalized medicine.

We recognize that with this vision comes immense responsibility to the millions of individuals who have chosen to participate in something larger than themselves. We are here today not only to answer your questions, but to reaffirm our deep commitment to data privacy and security, transparency, customer choice, data stewardship, and scientific integrity.

Founded in 2006, 23andMe is a personal genomics and biotechnology company that pioneered direct-to-consumer genetic testing. We are named after the 23 pairs of chromosomes in every human cell. Our mission has always been to empower consumers by providing access to information about their personal genetics based on the latest science so that they can make their own informed decisions about their healthcare journey.

Our services allow customers to gain DNA insights about their genetic risk for dozens of conditions like type 2 diabetes, Alzheimer's disease, and certain cancers. They can also learn about their carrier status for inherited conditions like cystic fibrosis or Tay-Sachs disease, or wellness factors like lactose intolerance or deep sleep intolerance.

23andMe customers have consistently reported taking positive health actions after learning about their genetics through 23andMe's services. Eighty-two percent of our customers with an actionable genetic result were previously unaware of their health risks.

The value of personal genomics goes beyond the insights people learn about themselves. Customers who register for our services also have the option to allow their data to be shared for research purposes, and over 80 percent of our customers have chosen to consent to research.

Consent is a central tenet of 23andMe's research program. We have separate research consents beyond our consents to processing sensitive data, a privacy statement and terms of service that customers must review and agree to if they want to participate in our research program. We remove all identifying information before any genetic data is shared with third parties. Any customer who affirmatively consents to participate in our research program can easily opt out at any time through their account settings and have always been able to do so. Customers are also free to delete their account and data at any time.

Our customers who have affirmatively consented contribute to more than 230 studies on topics that range from Parkinson's disease to lupus to asthma and more. We collaborate with advocacy organizations, universities, and biotech companies to bring customers opportunities to participate in research. Since 2010, 23andMe has published 293 papers that help advance scientific research in a wide range of fields.

Due to circumstances that I discuss in more detail in my written testimony, 23andMe is currently conducting a sales process supervised by a United States bankruptcy court. That process has been a success to date. We have two remaining bidders, both American enterprises, that will conduct a final round of bidding later this week before the sale of the winning bidder is presented for approval by the bankruptcy court. Because this proceeding is ongoing, I am unable to speak about the merits of either bid or the ongoing sale process.

Let me assure the Committee that 23andMe remains committed to protecting customer data. We are requiring that anyone bidding for 23andMe must agree to comply with our privacy policies. We recognize the vital importance of protecting every individual's right to access and control their own genetic information. Empowering people with the knowledge about their DNA is not only a matter of personal autonomy, it is a gateway to proactive and personalized health, informed decisionmaking, and greater engagement in consumer and scientific progress.

At 23andMe, we believe that when consumers are trusted with their own data, they become partners in advancing medicine and not just patients of it.

I appreciate the opportunity to testify before this Committee today, and I welcome your questions.

[The prepared statement of Mr. Selsavage appears as a submission for the record.]

STATEMENT OF I. GLENN COHEN, DEPUTY DEAN AND PROFESSOR, HARVARD LAW SCHOOL, CAMBRIDGE, MASSACHUSETTS

Professor COHEN. Chairman Grassley, Ranking Member Durbin, other distinguished Members of the Committee, my name is Glenn Cohen. I'm a deputy dean and professor at Harvard Law School. I

work on the legal and ethical issues in medicine and the biosciences, including genetics. Thank you for the opportunity to testify before you today.

Genetic data requires special protection because it is immutable, it inherently identifies us, it reveals information about our blood relatives, and because many health conditions have significant genetic components, so knowing about someone's genes is knowing about their health. If one's genetic information was accessed, it might reveal information on prognosis for breast cancer, Alzheimer's disease, and many other health conditions. It might let people identify you, including reconstructing your face and vocal characteristics. You might face discrimination in life, disability, and long-term care insurance, and it might reveal misattributed paternity.

There are additional risks to our servicemembers. Indeed, the Pentagon warned that our enemies might use the 23andMe data for "mass surveillance and the ability to track individuals without their authorization or awareness." And that's just today's risks. The development of polygenic risk scores may further reveal our risk for various diseases, and some have begun using 23andMe data to create scores to predict behavioral traits like risk tolerance and even educational attainment.

Since 2006, through its direct-to-consumer genetic tests, 23andMe has amassed a vast data base that includes the genetic and personal information of more than 15 million consumers. For many, it also holds physical specimens like saliva samples. The main privacy protection for those customers is just a promise the company has made in its privacy statement not to share personal information voluntarily with insurance companies, employers, or public data bases, or with law enforcement agencies without a valid subpoena, search warrant, or court order.

But if you read more closely, the privacy statement provides much less protection than it appears to. Few customers read or understand privacy statements or terms of use. 23andMe reserves the right to alter the terms customers have relied on, and moreover, the company explicitly reserves the right to transfer customer personal information in the event of the sale of the company or a bankruptcy.

The company has announced as part of the bankruptcy process it will "require anyone bidding for 23andMe to agree to comply with our privacy policies and all applicable privacy laws." Well, that's all well and good, but even if that becomes a condition of the sale, nothing prohibits Regeneron, TTAM, or another buyer of the data from altering that privacy policy just as there's nothing to stop 23andMe from doing so tomorrow. It's also unclear to me what's going to happen to the saliva samples, raising additional privacy concerns.

Trust is all about a relationship. Customers who chose 23andMe entered into a particular kind of relationship with a particular kind of company. They shared their genetic and other personal information, recognizing there was some privacy risk to obtain potential ancestry and health-related insights, and for some of them to help enable research and the development of potential new drugs or other therapeutics.

Upon bankruptcy or sale of the assets, consumers may find themselves in a relationship with a very different kind of company with goals they may not support and policies that have changed while they weren't looking. Privacy statements and customer acquiescence have a role to play, but private ordering solutions can only go so far to deal with these concerns.

And Federal law is not currently up to the job. The Health Insurance Portability and Accountability Act, HIPAA, our main health privacy law on the Federal level, will not apply to 23andMe because it's not a covered entity. The Genetic Information Nondiscrimination Act of 2008 protects individuals from genetic discrimination for employment or health insurance, but unlike its equivalent in many of our peer countries, it doesn't cover life, disability, and long-term care insurance. It excludes military personnel and excludes protection for individuals on the basis of conditions that have already manifested in the individual.

In my written testimony, I've analyzed a series of possible alternatives for you to consider, but I want to focus on two here, two that I think are particularly promising. First, the Don't Sell My DNA Act introduced by Members of this Committee, Chairman Grassley, Senators Cornyn and Klobuchar, which would introduce a strong model of affirmative consent upon bankruptcy. We've heard a lot about consent from the company, and the question is, why aren't they getting consent at this moment for the transfer? Why not go back and ask people to affirmatively consent to that transfer? And that is what your act would help do. I would like to see it extended, in fact, beyond the bankruptcy to other forms of sale or transfer of genetic data and more explicitly cover the biospecimens.

The second complementary model I want to highlight is from Florida, which in 2020 became the first U.S. State to ban insurers from discriminating on the basis of genetic information in areas not covered by GINA, life, long-term care, and disability insurance. I would like to see a similar effort on the Federal level because when it comes to—I respect federalism, but when it comes to genetic discrimination, really, all Americans should have this protection.

Chairman Grassley, Ranking Member Durbin, and Members of the Committee, I'm appreciative of your focus on this important issue, and I thank you for the opportunity to testify before you today, and I look forward to answering your questions. Thank you very much.

[The prepared statement of Professor Cohen appears as a submission for the record.]

Chairman GRASSLEY. I am going to open up the Senate. Senator Cornyn, would you Chair while I am gone? I will be gone about 15 or 20 minutes. Thank you.

Go ahead, Professor Gotberg.

STATEMENT OF BROOK GOTBERG, PROFESSOR OF LAW, BYU LAW SCHOOL, PROVO, UTAH

Professor GOTBERG. Okay. Thank you for the opportunity to present to you today.

Chairman GRASSLEY. Push the button.

Professor GOTBERG. Thank you. Thank you for the opportunity to present to you today. I'm happy to provide some perspective on the sale of personal consumer data in bankruptcy. And the main message that I'd like to convey is that the concerns that you've raised are not inherently bankruptcy issues. I'd also like to advise against passing bankruptcy-specific prohibitions on the sale of data, and I'll explain.

Bankruptcy provides a vital public policy role in the smooth running of our economy. Bankruptcy is not inevitable when a company becomes insolvent, but its primary purpose is to mitigate and manage the losses caused by a debtor's insolvency. When a company becomes insolvent, the creditors of that company are obligated to engage in a competition for those debtors' limited assets. This competition looks like a race to recover their legal rights. This is the metaphorical or actual race to the courthouse.

The race imposes costs on creditors who have to expend resources, sometimes fruitlessly, because they have gotten there too late after the money has run out. Also, a piecemeal liquidation of the debtor's assets frequently devalues those assets or destroys value so that creditors are ultimately paid less. That's why we want parties to choose bankruptcy when the debtor is insolvent.

Bankruptcy isn't a haven for any party to avoid the enforcement of outside laws. This is a primary issue in the 23andMe bankruptcy right now to determine if there are State laws that would prohibit the sale of assets in that bankruptcy. But we also don't want parties to avoid bankruptcy because of specific laws that arise only in those instances.

If a company cannot sell assets in bankruptcy, it will simply do so outside of bankruptcy, without the benefit of court oversight or the transparency provided by bankruptcy proceedings and probably for a lower price. This won't actually protect consumers from the sale of their data. It will just deny them these protections that bankruptcy is intended to give. The primary advantage of bankruptcy is its efficiency and its ability to maximize the value of debtor's assets.

Federal law shouldn't protect consumer data only in bankruptcy proceedings. To the extent that Congress wants to prohibit the sale of personal consumer data, it should do so both inside and outside bankruptcy to prevent the strategic use of bankruptcy for reasons that have nothing to do with the efficiency of the proceedings.

I'm happy to answer any questions about this or any bankruptcy-related issues, but I would really encourage the Committee to consider holistic and universally applicable prohibitions to the extent they exist. Thanks.

[The prepared statement of Professor Gotberg appears as a submission for the record.]

Senator CORNYN [presiding]. Mr. Klein.

STATEMENT OF ADAM KLEIN, DIRECTOR AND SENIOR LECTURER, ROBERT S. STRAUSS CENTER FOR INTERNATIONAL SECURITY AND LAW, (UT AUSTIN), AUSTIN, TEXAS

Mr. KLEIN. Mr. Chairman, Mr. Ranking Member, and Members of the Committee, thank you for inviting me to testify today.

Before joining the University of Texas, I served as chairman of the United States Privacy and Civil Liberties Oversight Board, an agency that Members of this Committee oversee and know well. Many of our oversight projects revolved around the insights that intelligence agencies can gain from personal data. That is because data is not just another commodity. When our adversaries buy or steal sensitive American data, they use it to harm the United States. China, in particular, has used American data to strengthen its military, conduct hostile intelligence operations, and help its companies displace American competitors.

Genomic data, like the DNA profiles held by 23andMe, presents several distinct national security risks. First, China could use DNA profiles to identify and track people of interest, such as American intelligence officers and critics of the CCP, the Chinese Communist Party, who live in the United States. China has already built a genetic data base to track and identify members of its Uyghur minority. With our genomic data, it could do the same for Americans.

Second, access to American genomic data could help Chinese biotech companies gain an unfair advantage over American companies. It could also help China train specialized AI models for biomedical research. Now, China has domestic AI datasets, but its population is far less genetically diverse than ours, so American genomic data would hold great value for them.

Third, China could use American genomic data for bioweapons research. Now, that risk is speculative, but it can't be dismissed. My written testimony lists several clues that China might be open to this kind of research. For example, a Chinese military textbook speculated about bioweapons designed for specific ethnic genetic attacks. Access to American DNA profiles with their greater genetic diversity could facilitate research into ethnically targeted bioweapons.

There is a disturbingly high chance, as Members of this Committee know, that we will find ourselves in an armed confrontation with the People's Republic of China before the decade is out, most likely over Taiwan. If so, we should expect China to target our homeland with unconventional, asymmetric tactics, which could include biologic attacks.

Next year, this Committee will once again consider Section 702 of the Foreign Intelligence Surveillance Act. As you do so, I respectfully encourage you to keep in mind that law's vital role in detecting adversarial plots against our homeland and stopping cyber intrusions into sensitive systems, potentially including systems like 23andMe's that store Americans' data.

I'd like to conclude on a positive note. In recent years, Congress, including this Committee and Members of this Committee and the executive branch, have done a great deal to protect Americans' data from hostile foreign powers. And as this hearing illustrates, leaders are now vigilant about the security risks of letting adversaries buy our data. For those reasons, I'm confident that the executive branch would block and could block an adversary-controlled entity from buying 23andMe. But the attention of this Committee and others in Congress is vital to help ensure an outcome to this bankruptcy that protects the privacy and security of Americans.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Klein appears as a submission for the record.]

Senator CORNYN. Thank you all very much. We will start with the 5-minute rounds of questions, and I will begin.

So back in 1990, Congress authorized something called the Human Genome Project, which was designed to map the human genome, which gave rise to an incredible amount of information about the human genome, which is what makes us who we are. And it has had enormous positive benefits in terms of law enforcement, for example, being able to use DNA as an essential part of regular criminal investigations to identify an assailant. For example, in a forensic analysis of a rape kit, it can identify with virtual certainty the perpetrator of the crime.

But at the time, it was also recognized that there could be tremendous abuse of that information. And indeed, we have touched on some of those, for example, discriminating against people based on their genetic profile for insurance purposes. For example, if you apply for life insurance or something of that nature and someone had access to your genetic profile, they could basically deny you because of perhaps some indication, some evidence of a genetic defect that would lead you to contract a disease or the like. And then, of course, employment, where there could be discrimination by employers against people based on their genetic profile.

So all of this is something we have anticipated to some extent, but I don't think we have been able to predict the extent to which this genetic profile, this genome data can be subject to not only beneficial use, but also use by our adversaries and for improper purposes.

Mr. Selsavage, did 23andMe do the actual testing of the saliva samples that were submitted by the people who engaged your company and your product?

Mr. SELSAVAGE. We contract with LabCorp, which is an American-based testing company to do the testing of the DNA samples for 23andMe.

Senator CORNYN. For all of it?

Mr. SELSAVAGE. For all of our testing, yes.

Senator CORNYN. And to your knowledge, is LabCorp—are there efforts to attack or to basically do cyber attacks on the data base that LabCorp maintained of 23andMe genetic samples and data?

Mr. SELSAVAGE. I am not aware of any particular cyber attacks on LabCorp. However——

Senator CORNYN. Well, you are not saying that LabCorp was somehow immune from cyber intrusions or cyber attacks, right?

Mr. SELSAVAGE [continuing]. No, I'm not, Senator.

Senator CORNYN. So can you tell us, as you sit here today, whether any of the genetic material that LabCorp tested that was collected by any of our adversaries or by criminal organizations, can you tell us with certainty that all of it was protected?

Mr. SELSAVAGE. To the best of my knowledge, you know, that data has been protected by LabCorp, and there has not been any breaches at LabCorp which has affected our data.

Senator CORNYN. Professor Cohen, generally speaking, if there is genetic information supplied along the same lines as 23andMe,

what is to protect individuals from outsourcing of some of that testing to, let's say, labs in China?

Mr. COHEN. I don't think there's much, Senator.

Senator CORNYN. And Professor Klein, you said this is a national security vulnerability. Why is that? Why would China, the Chinese Communist Party, want the genetic information on Americans?

Mr. KLEIN. Well, there are several potential uses, none of which are good. One is to use genetic information as a means of tracking and identifying people, something that every intelligence service and law enforcement agency——

Senator CORNYN. And that could include the active-duty military?

Mr. KLEIN. Active-duty military, intelligence officers working for the United States, Chinese dissidents who are living here and have come here to enjoy freedom and freedom of speech but whom the CCP is tracking.

But then looking forward into the age of AI, having large datasets with genetically diverse populations represented in them is very attractive for training specialized AI models. We know we're in a fierce competition with them, and we need to keep these advantages for American companies and for the U.S. Government.

Senator CORNYN. And would each of you agree with me that the genetic information that is collected through one of these saliva samples by a company like 23andMe doesn't just tell you something about the person who provides that saliva sample. It tells you something about their parents, about their children, and about their grandchildren, and anybody who might be a genetic relative of that individual.

Professor COHEN. That's right, Senator. When we say 15 million, that is kind of an underestimate when you think about all of these generations of people who are affected.

Senator CORNYN. Senator Durbin.

Senator DURBIN. So it seems to me that 23andMe tried, Mr. Selsavage, to come up with a policy to protect its consumers, but there is little to guarantee that the next buyer or the one after that won't abuse that policy, is there?

Mr. SELSAVAGE. Senator and Ranking Member, 23andMe has required as part of the sale of the assets of the company that any buyer of the company must comply and adopt the privacy policy and consents that 23andMe have in place today.

Senator DURBIN. So I didn't think I would ever say this in this room, but does the rule against perpetuities apply?

[Laughter.]

Mr. SELSAVAGE. Congressman, can you clarify that for me?

[Laughter.]

Senator DURBIN. I have tried to forget every aspect of that course in law school, but what I am suggesting to you is two or three buyers removed, your best intentions don't mean much, do they?

Mr. SELSAVAGE. Senator and Ranking Member, you know, my understanding is that, you know, 23andMe is doing everything we can to ensure that the next buyer adopts the policies and consents of 23andMe, and, you know, while I can't actually testify to their future intentions, both are, you know, American institutions with

experience in genomics, and, you know, are committed to protecting that data and continuing——

Senator DURBIN. Unless we have a Federal law relative to this issue that applies to future transactions, your best intentions don't mean much, as far as I am concerned. And don't take it personally.

So, Professor Cohen, there was a best-selling book a few years ago called The Immortal Life of Henrietta Lacks, fascinating book, story of an African-American woman who died in 1951 of cervical cancer in Baltimore if I am not mistaken. A sample of her tumor generated what is known as the HeLa cell line. That cell line was mass-produced and sold to laboratories all over the world. It has been used in scientific research, including research into cancer, the human genome, and the development of the polio vaccine. It is still being used today. Famously, Henrietta Lacks never consented to the use of her cells in this way, and despite the vast sums of money the cell line has generated, her family has never seen a dime of profits.

Part of what is being sold by 23andMe is a collection of biological samples submitted by consumers who wanted their DNA examined. They may have consented to some use of their samples, but I question how informed it actually was. And there is no guarantee a new owner won't change how the samples are used. Are you familiar with this story?

Mr. COHEN. I am, Senator.

Senator DURBIN. Is there anything we can learn from it in this application?

Professor COHEN. I think to learn for the importance of affirmative consent, and again, affirmative consent that can explain as much as possible what you want to do with material. And again, we still haven't heard an answer why at this stage they're not going back to all of their customers and asking, can you consent to the transfer of your data to this new buyer? It's a very simple thing that the company could do. Why aren't they doing it?

Senator DURBIN. Mr. Selsavage, why aren't you doing it?

Mr. SELSAVAGE. Senator, 23andMe believes we've obtained the consent from our customers, and when the customer signed up to our—to the service, they have agreed affirmatively to consent to our privacy and terms of service, which specifically says that we—in the event of a bankruptcy sale, that we can actually transfer their data.

Senator DURBIN. I think what Professor Cohen is suggesting is that there is more that could be done to protect your consumers. Would you consider it?

Mr. SELSAVAGE. I can take that suggestion back to our team, Senator.

Senator DURBIN. I hope you will.

Professor Gotberg, I guess my conclusion from your testimony was the bankruptcy code really didn't envision what we are talking about here.

Professor GOTBERG. So the bankruptcy code treats—it respects law that exists outside of bankruptcy just the same in bankruptcy proceedings as outside, so any legal prohibitions that apply outside bankruptcy also apply inside bankruptcy. So in a way, the bankruptcy code did anticipate that. It just doesn't introduce new sub-

stantive law when a company files for bankruptcy. There's not new prohibitions that exist.

Senator DURBIN. But what you say is, in your testimony, current bankruptcy law provides some oversight that can prevent the worst privacy policy abuses in a bankruptcy sale, but it does not prohibit the sale from taking place. Placing a prohibition on bankruptcy sales would simply push them outside bankruptcy proceedings where there are fewer protections. The best policy would make any restrictions on the sale of personal consumer data universally applicable. It is time for us to legislate, isn't it?

Professor GOTBERG. I would say if you want to protect consumers from having their personal consumer data bought and sold, you need to do that.

Senator DURBIN. Amen. Thank you, Mr. Chairman.

Senator CORNYN. Senator Durbin, we have seen history made today because in your long and distinguished career in the U.S. Senate, I know you have been waiting to use the phrase rule against perpetuities in a question, so congratulations for that.

[Laughter.]

Senator CORNYN. Senator Blackburn.

Senator BLACKBURN. Thank you, Mr. Chairman.

Mr. Selsavage, I want to ask you—let me say this. We all know that China is hard at work trying to build a virtual you of each and every one of us, and this is why we need to have a Federally preemptive online privacy law, which we do not have. And whether it is 23andMe and genetic information or whether it is data security, this is something that we need. But you seem a bit naive to think that you haven't had any breaches or any attacks, cyber attacks. Our critical infrastructure in this country is hit many times a day.

So what I want you to do—and you can submit this in writing—is to go into detail about how you anonymize and how you mask consumers and their information. And you can submit that during the QFR period. But I think it is important that you lay this out so that individuals know what level of protection that they are going to have. You all may sell, and then there may be an immediate buyer. You sold to 23andMe. You thought that would be a longer-term relationship. It is not. And then there may be three or four subsequent buyers, so some certainty and some awareness would be a good thing. And I want that in writing. Thank you.

Mr. SELSAVAGE. Senator, thank you for that. And I will take that back to our team as well.

I do want to note that, you know, I'm clearly aware that, you know, basically there are many cybersecurity threats. And at 23andMe, security and our customers' privacy is top of mind. And, you know, basically, we, you know, at 23andMe, do have cybersecurity threats from our foreign adversaries and others. And I will take your concerns back.

Senator BLACKBURN. Thank you. I thank you for that clarification because we deal with that issue repeatedly and the severe threats that exist each and every day.

Okay. Mr. Klein, I want to come to you. Talking about a privacy standard, there are some States, including my State of Tennessee, who have stepped forward. And Tennessee, in 2023, enacted the

Genetic Information Privacy Act. That requires companies to protect consumers' private information and to provide them with the ability to access their data, to delete their data and their account, and to destroy their biological sample. However, not all Americans enjoy this protection. So in that regard, is the Tennessee law a model for moving forward?

Mr. KLEIN. Well, I haven't studied that law closely, Senator, but it certainly sounds appealing to me as a citizen, as a consumer. And I've been following the saga of the general Federal privacy law that everyone seems to want for many years now. And the Committee understands better than I do the challenges that have arisen in coming to an agreement on something that everybody seems to want.

I think what the bill that Senator Cornyn and the other Members have introduced demonstrates is that even as—and the Tennessee bill is that even as we wait for a general law, there is possibility of making progress on sector-specific issues. And in my testimony, I highlighted some of the very good things that the Committee and other parts of the Congress has done on this specific threat from hostile foreign actors. And I do think, to Congress' credit, we've tightened that up considerably in the past few years.

Senator BLACKBURN. Mr. Selsavage, the Tennessee attorney general issued a statement after you all filed for bankruptcy, issued a statement notifying Tennesseans of their right to request a deletion. So talk to me about how you were moving forward with these deletion requests.

Mr. SELSAVAGE. At 23andMe, any one of our customers at any time can delete their data. For our customers, it's a simple process. All they need to do is log into their account at 23andMe, go to their settings, and request their account to be deleted. That process is automatic. We do ask for their date of birth just as an additional verification measure. And we've complied with those deletion requests and over—you know, through—you know, through the bankruptcy process and prior to that.

Senator BLACKBURN. And when they delete their account, they are also deleting their biological sample. Is that correct?

Mr. SELSAVAGE. If a customer has consented to—for us to biobank their saliva sample, we will also delete and destroy that saliva sample——

Senator BLACKBURN. Thank you.

Mr. SELSAVAGE [continuing]. Upon their request to delete their data.

Senator BLACKBURN. I yield back.

Senator CORNYN. Senator Klobuchar.

Senator KLOBUCHAR. Thank you. I think I will start by following up with Senator Blackburn's good questions. And by the way, thank you, Mr. Klein, for mentioning the need for a general privacy bill, which we badly need.

So on this deletion issue, it is my understanding that 1.3 million consumers asked 23andMe to delete their genetic data. Many faces technical issues. So how long is the backlog right now? And what are you doing to make sure all the requests are fulfilled?

Mr. SELSAVAGE. Senator, the good news is that today there is no backlog, that we are current on all of the deletion requests. What

did occur, you know, is when we filed for bankruptcy and, you know, many State attorneys general requested—or suggested to consumers that they delete their data at 23andMe. We did receive a significant amount of deletion requests. We quickly added additional staff and, you know, basically were able to reduce that backlog.

Senator KLOBUCHAR. Thank you. And will you commit to ensuring that consumers will retain their right to have their genetic data deleted after the bankruptcy sale is completed by making deletion rights a condition of the sale?

Mr. SELSAVAGE. Both of the bidders and, you know, the bankruptcy sale of 23andMe, both Regeneron and TTAM Research Institute, have agreed to adopt the policies of 23andMe, the privacy policies——

Senator KLOBUCHAR. So the answer is yes?

Mr. SELSAVAGE. So, you know, the answer is yes.

Senator KLOBUCHAR. Okay. During the bankruptcy process, how is 23andMe ensured consumers could decide how information is used and for what purposes since that is what your website has promised consumers?

Mr. SELSAVAGE. Our consumers consent not only to a terms of service, a privacy policy, there are also separate consents for our customers to—if they so choose, to engage in research at 23andMe and yet a—and then a separate consent to allow us to engage with research with third parties. And, you know, we make sure that customers have the right to actually opt in. We don't default those. Customers are actually clicking yes, they will want to conduct—or enable their data to be used for research purposes. Many customers understand these are important for understanding disease and genetic conditions and lifesaving medical treatments.

Senator KLOBUCHAR. Thank you. Professor Cohen, it is my belief that the privacy policies aren't meeting the privacy needs of consumers during bankruptcy. That is why I have worked with Senator Cornyn. I appreciate his leadership, and Grassley, to give consumers control over their genetic data with our bill, Don't Sell My DNA Act. Why is it so important that we require consent from the consumer before their genetic data is sold to another company with which they have no prior relationship?

Professor COHEN. People are engaged in a trust relationship. You know, if my father gave me access to his medical records and says, son, I want you to look at this and be careful with this, and I went ahead and said, let me give it to somebody else without asking my dad, you'd look askance at what I was doing. The same thing is happening here. They're essentially transferring data and transferring a trust relationship to a new entity, and people have the right to know who they're dealing with and the right to consent to it.

Senator KLOBUCHAR. Do you believe that the right to control one's personal genetic information should take precedence over maximizing returns for creditors in a bankruptcy proceeding?

Professor COHEN. Well, I think that it would be nice for the creditors to get paid, Senator. In this instance, I think this information is so sensitive and so important, it's really important to protect people's information.

Senator KLOBUCHAR. Okay. Thank you. And Professor Gotberg, do you believe that the current consumer privacy ombudsman system in bankruptcy proceedings is sufficient to protect consumers' most sensitive information?

Professor GOTBERG. So the consumer privacy ombudsman is appointed to help the court in weighing the costs and the benefits of any particular sale of assets. If you permit consumer—privacy—personal consumer data to be sold outside of bankruptcy, it's permissible inside of bankruptcy as well. And so the consumer privacy ombudsman is just trying to weigh what would be the negative effects of that sale.

Without an understanding of the price of privacy, so to speak, that's a very hard balancing act to perform. To my knowledge, there's been no final litigation to determine what the damages would be for an individual to have their privacy violated in that way, so it makes it really hard for the consumer privacy ombudsman to have an effective role there.

Senator KLOBUCHAR. Okay. And sort of to end where I began with Mr. Klein's point, why is it so important that Congress enact a comprehensive privacy law? By the way, the same companies that were lobbying against one, because I am also on the Commerce Committee, say 10 years ago now want one because of the patchwork of laws that we now have in our States, which is very predictable, which I hope people will realize that we need some AI rules of the road in place and tech rules of the road in place. And it is just the worst, that people just think they can lobby against things, and then all of a sudden they are like, oh no. So tell me why we need a privacy law and how that would have helped here.

Professor GOTBERG. So a greater predictability for companies when they're entering into agreements with consumers would be—is always beneficial. So if companies know what the legal limitations are, then they can take that into account and creditors can take that into account whether an asset will be available before lending to the debtor. So it's important to have that law in place inside and outside bankruptcy.

Chairman GRASSLEY. Oh, I am sorry. I didn't mean to interrupt you. I thought you were done.

Senator KLOBUCHAR. Well, good. No, I am not going over my time. Done.

Chairman GRASSLEY. Senator Moody.

Senator MOODY. Thank you, Mr. Chair. And thank you for conducting this hearing and for all of our witnesses that have taken time to be here. These are complex issues and certainly we appreciate your expertise on the matter.

I think any American sitting at home when they learned of this bankruptcy that had submitted information to 23andMe was probably, you know, terrified and had never thought about what would happen to their information. So it is not just policymakers that are worried about this. I think people all around the United States are now concerned of what happens to their very sensitive personal information.

And I think this is going to affect everything from data privacy to national security to potential biotech threats. And we cannot overState the threat to this Nation and to people individually. I

think it is both going to be from a national security concern, but also private companies getting access to some of this data.

I appreciate the shoutout to Florida. Florida does lead in many of these policy areas. We are not afraid to diligently dig in and take action quickly to protect people and their rights, and thank you for acknowledging that. In fact, right now, as we sit here, it is not illegal for insurance companies, life, disability insurance to inquire about, get access to your genetic information in all 50 States except Florida, and so we appreciate that.

And I think it is going to be imperative that this body, as we are presented with the sale of companies that have access to this information—and it is not just 23andMe. There are going to be other companies that get access to genetic information to be used in business models, to develop strategies to maximize profits, whether that is from their everyday course of business or whether that is selling of assets. We are going to have to deal with how the exchange of genetic information of Americans is protected and whether it can even be treated as an asset.

And I want to start first, sir, we appreciate you being here, and I know you have the best of intentions, you have said, as it relates to the assets. And you consider the genetic information of Americans to be assets?

Mr. SELSAVAGE. The genetic information belongs to the consumers and—you know, basically, and it is a very valuable asset to those consumers, yes.

Senator MOODY. But to 23andMe, you considered that to be an asset?

Mr. SELSAVAGE. It is an asset to 23andMe, yes. I mean——

Senator MOODY. And in terms of valuing your business moving forward or valuing your particular parts of your assets in a bankruptcy, that is one core asset?

Mr. SELSAVAGE. Senator, we did not value that asset, you know, per se as part of the bankruptcy. However, the bidders are looking at that and placing a value on it.

Senator MOODY. A bidder wanting to buy your company is assessing whether or not they can buy that data as part of how much they are going to pay you?

Mr. SELSAVAGE. Yes.

Senator MOODY. And the more customers that delete their information, the less of that asset is available to transfer is what you are telling us today?

Mr. SELSAVAGE. Senator, you know, for us at 23andMe, we've let the buyer——

Senator MOODY. Yes or no. And you are deleting that data, and once you sell an asset off, will it be less of an asset to sell?

Mr. SELSAVAGE. There will be less customers with genetic information in our data base as people delete them, yes.

Senator MOODY. So the customers that don't get this notice across the United States, the warnings from the attorneys general that this is a problem, you need to delete your information, if they have moved and they don't get the notice and they don't delete it, they are part of the asset group that goes to the other country, right?

Mr. SELSAVAGE. Senator——

Senator MOODY. Or goes to the other—could be the other country, I am sorry, the other business.

Mr. SELSAVAGE. Senator, we have provided notice to all of our customers of the bankruptcy proceedings. And this week, we will be providing notice of the sale of the company to either Regeneron or TTAM Research Institute. And at all times, our customers have complete control over their data. They have the right——

Senator MOODY. Except for the ones that didn't get notice and don't know about the sale, right?

Mr. SELSAVAGE. Senator, with all due respect, we are doing everything we can to make sure all of our customers get that notice of the bankruptcy and of the sale. We are—we've emailed them——

Senator MOODY. I heard that you have the best intentions. So I am also hearing that we might need to modify Federal law to address these intentions because when you are talking about the sale, you list that you will not sell to any countries of concern on your website. But I guess all other foreign nations could presumably offer to buy, right, if they're not a country of concern in your mind?

Mr. SELSAVAGE. Senator, you know——

Senator MOODY. Yes or no? Your limiting the exclusion of those to countries of concern.

Mr. SELSAVAGE. We are limiting the sale of assets to any foreign adversary to the United States, any companies in those countries.

Senator MOODY. But another foreign adversary could buy this information—or excuse me, another foreign nation-state could buy this information and sell it to a foreign adversary. Nothing prevents that, right?

Mr. SELSAVAGE. Senator, with all due respect, we have only two bidders left here, and both are American enterprises. Both Regeneron is a public pharmaceutical company here based in the U.S. and TTAM Research Institute also is an American foundation, you know, founded by the former CEO and co-founder of 23andMe——

Senator MOODY. At the core of it, I understand you are saying right now there are only two bidders left, but under Federal law and under what your best intentions are permitting, it could have allowed for a foreign State to buy these assets, nothing would have prohibited that, and selling it to a foreign adversary, correct? Nothing in federal law would have prevented that.

Mr. SELSAVAGE. Senator——

Senator MOODY. Correct?

Mr. SELSAVAGE [continuing]. I am not a lawyer, but I do believe there are regulations, and there would have been different oversight if any of the assets were sold to anyone outside of the United States. And——

Chairman GRASSLEY.

[Off mic.]

Senator MOODY. Thank you, Chairman Grassley.

Chairman GRASSLEY.

[Off mic.]

Senator COONS. Thank you, Chairman Grassley, and thank you to each of the panelists for coming here today and testifying on this important issue. It is particularly valuable that you are here to shed light on two issues important to our Nation, to our families,

and frankly, also to my home State of Delaware, namely, bankruptcy and data privacy.

As I am sure some of you know, Delaware is the most popular State in our Nation for corporate incorporation, which also makes it a prominent bankruptcy jurisdiction. Delaware also is one of a small handful of States that has enacted robust data privacy protection laws, making it a potential model for federal legislation on data privacy, particularly in the context of bankruptcy.

I do think it is critical that we strike the right balance between safeguarding data and personal information and maintaining a bankruptcy system that makes creditors whole and gives debtors a fresh start.

If I might, Professor Gotberg, is a prospective buyer in bankruptcy legally required to follow 23andMe's current privacy policy?

Professor GOTBERG. So the privacy policy is a contract——

Senator COONS. Right.

Professor GOTBERG [continuing]. So contracts are enforceable as between the two parties. In law school we like to teach that a contract is a promise to perform or to pay damages. So a company that undertakes a contract, if they don't perform, would open itself up to a lawsuit for damages. That's true for 23andMe, and it would be true for any subsequent buyer. Whatever the buyer agreed to do would just be a contract. It wouldn't be—there would be no enforcement mechanism to force them to comply. They could just choose to breach.

Senator COONS. Nothing other than damages enforces that contract. And is there anything in the bankruptcy code that specifically addresses the transfer and use of highly sensitive personal data?

Professor GOTBERG. In that situation, that is where the consumer privacy ombudsman could be appointed.

Senator COONS. Could be.

Professor GOTBERG. Right, but in that situation, their role is primarily to advise the bankruptcy judge to weigh the costs and benefits of any potential breach of a privacy policy. So again, without being able to put a number on what that—those damages are, what the cost is for a violation of privacy, it actually becomes a pretty difficult weighing exercise.

Senator COONS. Is there any relevant precedent?

Professor GOTBERG. I don't know that it's ever been litigated. I haven't seen anything.

Senator COONS. Me neither. Professor Cohen, Delaware and a few other States have enacted strong data privacy laws designed to regulate entities that control sensitive data, give individual consumers the right to access, correct, or delete certain data. How can my colleagues and I do something similar at the federal level and specifically in the bankruptcy context to ensure sensitive data doesn't end up in the hands of the wrong people or the wrong country as a result of a bankruptcy proceeding? And what is your view on the Don't Sell My Data Act where I have joined Senators Grassley, Cornyn, and Klobuchar as a co-sponsor?

Professor COHEN. So I think the Don't Sell My Data Act is exactly the right idea here. I will say that I think that the—what's important is this idea of affirmative consent. That's what is central

to the bill upon the transfer. And again, we still really haven't heard a good reason why we can't go back to all of these people and ask them, can you affirmatively consent to the transfer of your data to Regeneron or TTAM? So I would love to see Congress push that and push it beyond bankruptcy to other kinds of sales of information as well.

Senator COONS. Let me ask you a question about affirmative consent. Part of the market value of 23andMe is a service that is individually genetically identifying that gives you information about, honestly, one of the most private things there could be, which is whether or not you are susceptible to certain diseases, what is your genetic ancestry, that sort of thing. Would it not stand to reason that although logistically challenging, going back to every individual who has given their personally identifying genetic information to 23andMe and affirming their consent would actually, in the end, build their market value by reinforcing that this kind of a service is something where people can count on it to protect their data privacy, regardless of whether there are damages available?

Professor COHEN. I think if you build your company on a reputation of trust and a reputation of autonomy and empowering people, this is exactly the thing you want to sell to customers to say, we believe so much in what we say that we're even going to do this upon sale or bankruptcy.

Senator COONS. And I understand how it might be complex or expensive, but in the end, I think it ultimately serves the entire segment of personally identifying genetic consult because it builds trust.

Thank you, Mr. Chairman. Thanks for a chance to question.

Chairman GRASSLEY. I will take my turn now. I am going to start with Mr. Selsavage.

In 23andMe's March 23 press release, the company indicated that data privacy would be "an important consideration in any potential sale." But when there was a motion to appoint a consumer privacy ombudsman in the bankruptcy, 23andMe first opposed the appointment of an independent ombudsman to ensure that genetic data was protected in the sale. Why did the company oppose appointing a privacy ombudsman?

Mr. SELSAVAGE. Yes, Mr. Chairman, 23andMe was the first to suggest that the bankruptcy court appoint a customer data representative, which would look at the privacy issues in this particular bankruptcy case. 23andMe, at the time, did not believe that a consumer privacy ombudsman was needed. And the reason—the differentiation there is a consumer privacy ombudsman is required in bankruptcy when, you know, there's a change in the privacy policy from one company to the next.

In this particular case, you know, we, as part of the bidding process for 23andMe, were requiring that any company that was considering acquiring 23andMe's assets, including its data base and our customers, would be required to retain the privacy policies and consent going forward.

Chairman GRASSLEY. I think that answers that question. So is 23andMe's priority to sell consumer genetic information to the highest bidder or to ensure that the genetic data it has collected will be protected according to existing privacy policies?

Mr. SELSAVAGE. Mr. Chairman, our customers' data and privacy is, you know, a top priority in this process, you know, at 23andMe and for the special committee overseeing this process. It is not just the highest bidder. We are—have required that, you know, basically any bidder, as I said, and the two remaining bidders have affirmatively said that they would actually continue those privacy policies and consent and put that in writing in their asset purchase agreements or contracts to buy the company.

Chairman GRASSLEY. Also to you, the point of bankruptcy is to "marshal assets in a way that maximizes their value for the benefit primarily of creditors and then once creditors are paid for owners." And in your written testimony, you agree with the aim of maximizing the value of the business for stakeholders, but placing as little restrictions on the customer data as possible makes the data more valuable to the buyer. Would you characterize genomic data as a bankruptcy asset?

Mr. SELSAVAGE. Mr. Chairman, you know, I believe that the genomic data is an asset and, you know, we have—23andMe is treating it—and not only maximizing the value for our creditors and our shareholders, but also, you know, one of the most important pieces—parts of 23andMe is our customers and our customers' trust, and we are putting their privacy and their security as part of that process and it is top of mind for the company and special committee overseeing this process.

Chairman GRASSLEY. Okay. Based upon your "yes" answer, isn't your duty to protect consumer data in tension with your duty to maximize the value of the estate asset?

Mr. SELSAVAGE. I think we are looking at both of those duties combined, Mr. Chairman.

Chairman GRASSLEY. So I think you are saying that consumer data doesn't have a higher value than the estate. So aren't you a little bit in conflict with some other things you said here?

Mr. SELSAVAGE. You know, basically protecting our consumers' data and their privacy and their consents as part of this process is a large consideration and, as I mentioned, it is not just accepting the highest dollar amount for the assets.

Chairman GRASSLEY. My last question will be, Mr. Klein, in 2019, the DOD advised members of the armed services not to use direct-to-consumer genetic testing devices. The guidance noted the risk of mass surveillance and the ability to attract individuals without authorization. How could foreign adversaries use either the personalized or the aggregated genetic information of U.S. servicemembers to harm U.S. interest in military operations?

Mr. KLEIN. Thank you, Senator. Well, we know that intelligence services and police agencies like the FBI use genetic data to identify people of interest, and foreign adversaries certainly have a great interest in members of our military, where they go, what they do. So that would certainly be a concern for me, and we can be assured that they are looking at that and trying to use our servicemembers' genetic data.

You also mentioned aggregate. Large datasets have great value today for training AI models. China is trying to build large datasets in every conceivable area, but they have some gaps. One of those gaps is that their population is not genetically diverse, and

so they may have a large number of DNA profiles in their country, but they don't have the diversity that we have. And that genetic diversity is very helpful if you want to train a model that is predictive for things benign, like biomedical research, but also things malevolent, like bioweapons research. We don't want them to build out their data base of DNA profiles with the diverse and rich datasets that we have here in America.

Chairman GRASSLEY. Senator Schiff.

Senator SCHIFF. Thank you, Mr. Chairman.

Professor Gotberg, California has already passed legislation that went into effect in 2022 requiring direct-to-consumer genetic testing companies like 23andMe to obtain Californians' express consent for the collection, use, or disclosure of their genetic data. Under this law, Californians are also able to delete their accounts and genetic data and to destroy the biological samples they provided to these companies.

In the context of 23andMe's bankruptcy, can Californians still exercise these deletion rights, or does the bankruptcy process somehow interfere with, override, or otherwise affect our State's privacy protections?

Ms. GOTBERG. Thank you. Bankruptcy proceedings do not override any applicable law. So State law and Federal law are recognized in bankruptcy proceedings. Whatever rights your consumers have outside bankruptcy, they'll have inside bankruptcy in terms of their legal rights.

Senator SCHIFF. And if the data base, 23andMe's data base, is sold as a bankruptcy asset, what obligations would the acquiring company have under Federal or California law to maintain those same security standards?

Ms. GOTBERG. So the same laws that would apply now to 23andMe would presumably apply to any buyer.

Senator SCHIFF. And so even if this is not a California company operating in some other State, they would still be bound post-bankruptcy to California's privacy standards?

Ms. GOTBERG. To the extent that California privacy standards apply, yes, they would.

Senator SCHIFF. And is a commitment made by an acquiring company somehow enforceable, apart from California's law, vis-à-vis residents of other States, is a promise made by an acquiring company somehow legally enforceable, or is it only as good as the person's intention to comply with that commitment?

Ms. GOTBERG. So contractual promises are enforceable up to the point that they can be enforced. That's not a great answer, but again, our statement is a contract is a promise to perform or to pay damages. It's possible for parties to breach that agreement, in which case the party that—on the other side of it would be entitled to damages for the harm that they've experienced. But without——

Senator SCHIFF. You know, let's say I am acquiring 23andMe's dataset. I commit to maintaining the deletion provisions, et cetera, complying with California law even if it is not required somehow. I acquire the dataset, I don't comply——

Professor GOTBERG. Right.

Senator SCHIFF [continuing]. Has my offer to comply or my commitment pre-bankruptcy, has that somehow turned into a binding

contract with the owners of the genetic data, the people who have the genetic data?

Professor GOTBERG. So it would depend on who you were in privity with, I guess, in terms of the contract, to use, I guess, a fancy legal term. A contract is between two parties, and so you have to have an agreement between those two parties. And I guess the question in those situations, if you were promising to abide by the commitment, who would be on the other side of that promise? Who would be able to enforce it?

Senator SCHIFF. Right. Well, it would sound like the consumer would not be on the other side of that promise. It would be more one of the parties to the bankruptcy, which then we would be then relying on them to enforce that promise. Does that analysis make sense?

Professor GOTBERG. That makes sense to me.

Senator SCHIFF. And what controls are in place, Mr. Selsavage—maybe I can ask you this question. What controls are in place to prevent any unauthorized access or misuse of information during the bankruptcy proceedings?

Mr. SELSAVAGE. 23andMe is—you know, basically places data security and data privacy as top of mind. You know, we basically have continued to maintain a strong system of security, making sure all of our data is encrypted. You know, the genetic data is stored separately from any consumer identifying information identifying who that genetic data belongs to. We have enhanced our security processes, especially around bankruptcy, understanding that there is additional threats. And, you know, basically from—on the consumer side, you know, we have since enacted two-factor authentication to access—so basically, there is a second level of either an SMS text message or an email verification when somebody is trying to access their account and then placed additional restrictions if sensitive——

Senator SCHIFF. If I could just interrupt with one last question because my time is going to expire. How do we know that an acquiring company or entity or person would maintain the same security standards that you have over privacy and even those standards were subject to hack?

Mr. SELSAVAGE. Senator, the good news here is there is two potential buyers at this point for 23andMe. The first is Regeneron, an American $55 billion market cap pharmaceutical company who actually has data security over genomic data today. And TTAM Research Institute would be—which would be maintaining the same security standards as 23andMe.

Senator SCHIFF. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Britt.

Senator BRITT. Thank you, Mr. Chairman.

To followup on the Senator's question, so would you commit today to the same privacy standards that you have demanding those of the company that purchases 23andMe? Do not sell unless they keep the same privacy standards that you have?

Mr. SELSAVAGE. Yes, that is a requirement, you know, basically of any—of the two buyers, and they have put that in their asset purchase agreement.

Senator BRITT. Excellent. And tell me, what all do you test for?

Mr. SELSAVAGE. You know, 23andMe tests for, you know, basically a significant level of, you know, genetic traits, ancestry, and health conditions. We actually, as part of our process, test over 600,000 variants through our testing process.

Senator BRITT. Okay. So you are able to tell somebody maybe it is predictability of potential disease and other things?

Mr. SELSAVAGE. And while we can't definitively say that that person will get the disease, we can highlight risk—and basically when people are at higher risk for certain diseases.

Senator BRITT. And so do you test for sex?

Mr. SELSAVAGE. You know, as part of our testing, we do identify if the DNA showed that the—if the individual is male or female.

Senator BRITT. And male is XY chromosome?

Mr. SELSAVAGE. That is correct.

Senator BRITT. And female XX?

Mr. SELSAVAGE. Correct.

Senator BRITT. On your data base though, you go into saying that if people self-identify of another gender, that you will attempt to give them a prognosis of the gender that they identify with versus the gender that they test for?

Mr. SELSAVAGE. Senator, I'm not aware of that——

Senator BRITT. Oh, yes, you do. So it says, "We understand that sex is not always binary and the words male and female may not accurately reflect an individual's identity. We also recognize that being categorized by birth sex may be an uncomfortable or triggering experience to some, and we do not mean to delegitimize anyone's gender identity or expression. We use your self-reported sex to customize your health and trait reports. For example, genetic risk and what they may mean differ between men and women." So men and women are different, right? I mean, you say that here. We just talked about the genetic testing.

But then you go on to say, "If you tell us you are female, your reports will contain information that is relevant to genetic females XX. If you tell us you are male, your reports will contain information that is relevant to genetic males XY. Additionally, there are some sex-specific reports that are available on individual selected profile sex such as male hair loss or bald spot. That is because either we are not able to build out an acceptable model for both genders or because the trait is actually sex-specific."

And so I guess I am wondering, did you test—like if it is a genetic female that identified to you as a male, would you test them for male pattern baldness?

Mr. SELSAVAGE. Senator, you know, we—as you mentioned, we actually do—the customer does report to us, you know, what they believe their sex is, and we test against that, as well as what we found in the DNA as—testing as well.

Senator BRITT. I think probably the DNA is what is best for predicting actual future disease or harm or what may come, good or bad, for the individual.

On that note, you have about 15 million customers. Is that right?

Mr. SELSAVAGE. That's correct.

Senator BRITT. Okay. Of that, how many are kids?

Mr. SELSAVAGE. How many are kids?

Senator BRITT. Yes.

Mr. SELSAVAGE. Senator, I don't know that number.

Senator BRITT. So you don't know. From what I read on your website, obviously, parents can agree to have their child's DNA tested. Is that correct?

Mr. SELSAVAGE. That is correct.

Senator BRITT. So you don't know? Of the 15 million people, you don't know how many of those profiles are under 18?

Mr. SELSAVAGE. I don't have that information with me today, but I'd be happy to take that back for——

Senator BRITT. Do you have a guess?

Mr. SELSAVAGE. I don't have a reasonable guess, Senator.

Senator BRITT. Sir, I think we have to be vigilant when it comes to children and their DNA. We have talked today about all of the potential risks that can occur from privacy to security risk, obviously, blackmail, amongst a number of things. Would you commit to me today that in the sell, you will sell no child's DNA under the age of 18, that you will delete that account?

Mr. SELSAVAGE. Congressman—or Senator, I will take that back and will review that.

Senator BRITT. I think you absolutely should. And on that note, when it comes to bankruptcy, Professor, tell me, you know, when you look at a privacy ombudsman in this space, when you are looking at minors, children, what type of protection is currently in place, and what do we need to be doing as Congress? And actually, I would like to open this up to everybody to ensure that children are protected in this space.

Professor GOTBERG. My understanding is that there are specific laws protecting children's information. I'm not an expert on those laws, but whatever laws exist outside of bankruptcy are enforced inside of bankruptcy as well.

Senator BRITT. Do you all have another—I would love your thoughts.

Professor COHEN. You know, for human subjects research, we have special rules for the children population, and that might be a place to look for some comparisons.

Senator BRITT. Do you have anything, Mr. Klein?

Mr. KLEIN. Well, as a father, I can say that I think we all struggle with how much of our children's data or how much of our children's lives to digitize, and so there's also a degree of parental responsibility. And when it comes to health, these are very tough choices sometimes for all of us.

Senator BRITT. Absolutely. Thank you, Mr. Chair.

Senator HAWLEY [presiding]. Senator Padilla.

Senator PADILLA. Thank you.

Now, colleagues, the witnesses today have explained that our bankruptcy process is primarily designed to maximize creditor payouts and ensure that a business, where possible, can continue to operate. It is not designed for other goals, but it is often called upon to fulfill other goals. Here, the bankruptcy process is not just required to protect consumer privacy, but also to protect our national security interests.

Professor Klein, what protections are built into the bankruptcy process to prevent foreign adversaries from taking advantage of the process to access sensitive information? Other concerns are gen-

erally raised, but, you know, we are talking about a specific area of the law, bankruptcy law here, whether we are talking about personally identifiable information or national security sensitive information?

Mr. KLEIN. Thank you for the question, Senator. And this is one area where there actually have been encouraging changes. We are not defenseless. In the FIRRMA law back in 2018, the Congress did give the Committee on Foreign Investment in the U.S. the ability to reach into the bankruptcy process and block sales and transactions, something that it previously hadn't had within its jurisdiction. As you all know, that body in the executive branch is one of our main protections against key intellectual property, sensitive data, and so forth, slipping out the back door to foreign adversaries.

Senator PADILLA. And how much of the sensitive information, if any, can potential buyers access before a sale becomes final? They are obviously doing due diligence in the process of making these decisions.

Mr. KLEIN. That is a great question, Senator. I would refer that to the bankruptcy experts on the panel.

Senator PADILLA. Anybody?

Professor GOTBERG. So can you repeat your question?

Senator PADILLA. How much access to this very sensitive information, whether it is personal sensitive information or national security sensitive information can a potential buyer access before a sale becomes final? Or is this an area where——

Professor GOTBERG. So there——

Senator PADILLA [continuing]. Legislative action is needed?

Professor GOTBERG. Within a bankruptcy proceeding, there is an allowance for due diligence. I think the procedures for that will be determined by the bankruptcy court and may differ from case to case. To the extent that there is no protections outside bankruptcy law, I don't know that there's—you know, bankruptcy law does not produce additional protections that wouldn't otherwise exist.

Senator PADILLA. So a potential area for needed congressional action is what I am hearing. Since we have an expert before us, at what point in a bankruptcy process can CFIUS get involved? And do you have any recommendations about whether they should be involved earlier in the process?

Professor GOTBERG. So I'm afraid you will have to explain what CFIUS is to me.

Senator PADILLA. All right, Then we have an expert here. It is okay. It is okay. We will do a followup with you because my time is limited. I want to get to another topic, which is national security and biotechnology. I recently served as a member of the National Security Commission on Emerging Biotechnology, and our findings in a recent report found that the United States has historically not treated biological data as a strategic asset like our agricultural base, our oil reserves, despite its importance in advancing biotechnology and AI.

Back to Professor Klein. What is your assessment of the CCP's effort to sweep up as much biological data that they can of Americans and of our allies and partners abroad to advance their own domestic biotechnology ambitions?

Mr. KLEIN. Well, I think we've seen, Senator—and thank you for the question—their ambitions are comprehensive. They want to dominate in critical sectors. They want to use information like this to enhance their military prowess, and potentially, and very worryingly, given the tension between our countries, to conduct asymmetric, unconventional attacks, potentially including biologic attacks.

I'm sure you all saw that just in the past 2 weeks, the Eastern District of Michigan U.S. Attorney's Office has indicted two separate sets of Chinese national defendants on smuggling biologic materials into the United States. We've also seen the report on the Reedley Biolab out of the House Select Committee where a person of Chinese nationality, citizenship, was in California running an unregistered biolab. We don't know exactly what was going on there.

Some of these reports are very disturbing. We don't have a complete picture, but we know that the system, as the 9/11 Commission put it, is blinking, if not red, at least dark orange, and we need to have the imagination—and I'm glad this Committee's doing it, to foresee how they might conduct unconventional attacks against our homeland in the event of an armed conflict.

Senator PADILLA. Do you have any recommended actions for this Committee or Congress as a whole to take to better protect our biological data while striking the important balance of promoting scientific research that depends on these datasets?

Mr. KLEIN. Yes, thank you, Senator. And bankruptcy is one vector. We're all covering down on that today. Cyber security, cyber attacks is another major vector. We know that it is very hard for companies to defend against a nation-state level attack, but we can at least make it harder for them. We can at least force them to expend their very best, most exquisite exploits to try to get in and spread those techniques that they have as thin as possible.

But I will also flag one other vector, insider threat. This is something that those of us who have led organizations in the Government dealing with classified material worry about every day, but it's also true in the private sector. Companies do not have the same comprehensive security clearance standards or personnel vetting standards that government organizations are supposed to.

There are some private sector actors that are starting to help, for example, defense industrial-based companies do this, but if an insider who has authorized credentials inside a company wants to take out a bulk dataset, whether it's genomic data or weapons designs, what does that company have in place to prevent that exfiltration? That's another very problematic vector.

Senator PADILLA. Okay. Thank you so much.

Thank you, Mr. Chair.

Senator HAWLEY. Mr. Selsavage, if I could just start with you. So how many customers do you have approximately?

Mr. SELSAVAGE. Between 14 and 15 million customers.

Senator HAWLEY. Between 14 and 15 million. I think you told Senator Britt just a minute ago that a goodly number of those are minors. Is that correct?

Mr. SELSAVAGE. What I said was I don't have the number of customers that are——

Senator HAWLEY. You have the genetic data of a good many minors. Is that correct?

Mr. SELSAVAGE. We have genetic data for a particular number of minors, and I will be providing—happy to provide——

Senator HAWLEY. People under the age of 18. Is that correct?

Mr. SELSAVAGE. That is how I am defining a minor.

Senator HAWLEY. So your customers—I just want to make sure I understand your business model. Your customers give you their genetic information for you to run various tests on. Is that right?

Mr. SELSAVAGE. Yes, that is correct.

Senator HAWLEY. And I mean, that is pretty sensitive stuff, isn't it, somebody's genetic information? Is there anything more personal than that?

Mr. SELSAVAGE. I would agree with you, Senator, that genetic data is sensitive information.

Senator HAWLEY. And so now you are just going to sell all of it, 15 million people, bunches of kids, maybe millions. It is just going to be sold in the open market?

Mr. SELSAVAGE. Senator, you know, the good news, as I mentioned, is that the two bidders are buyers for the company. One is Regeneron, which is an American company.

Senator HAWLEY. That is the big pharma company?

Mr. SELSAVAGE. Big—it is a——

Senator HAWLEY. It doesn't make me feel any better.

Mr. SELSAVAGE. It is a large pharmaceutical company.

Senator HAWLEY. All right. So you are going to take 15 million Americans' genetic information, and you are going to sell it to somebody. And your message to us is today, trust us, it will be fine. Maybe it is a big pharma company. Maybe we will get lucky. Maybe they will treat it right. I thought your privacy code, your privacy commitment said that consumers had a right not to have their information shared with anybody else without their consent. I mean, I have got your privacy statement right here. It says that without their consent, you can't share their information. You are about to sell it.

Mr. SELSAVAGE. Senator, that consent is, you know, essentially for, you know——

Senator HAWLEY. Not real?

Mr. SELSAVAGE [continuing]. Not shared for research purposes, and we are not selling it for research purposes.

Senator HAWLEY. Ah, so when you tell the consumer, give us your personal information, and we will take money from you, and we won't give it to anybody without your consent, it is not real. It just means, you know, maybe kind of depends on the day.

Mr. SELSAVAGE. Senator, you know, I will say that our customers' data is their own. They have the right at all times to access that information. They can edit it——

Senator HAWLEY. Well, sure they can, but you are about to sell it to who knows who. They can't control it. You said to Senator Moody that consumers have complete control of their data, complete. How can they have complete control if you are about to sell it without their consent?

Mr. SELSAVAGE. Senator, they can delete that data anytime up until the sale and after.

Senator HAWLEY. Oh, Okay. Okay. They can delete the data. Have you fixed the ability of customers to go on your website and delete it? Because right after you announced your sale, your deletion page went down. I hold in my hand here an article from The Wall Street Journal. "23andMe's site goes down as customers struggle to delete their data." Can they even get onto your site to delete their data?

Mr. SELSAVAGE. They can, Senator, and——

Senator HAWLEY. You fixed this?

Mr. SELSAVAGE. That was an issue that—yes, we fixed immediately after——

Senator HAWLEY. It is up and running now? Customers can go on?

Mr. SELSAVAGE. Customers can go on, and they can delete their data——

Senator HAWLEY. What happens when they go onto your site to delete their data?

Mr. SELSAVAGE. When a customer logs into their account at 23andMe, they go to their settings page, and they—there's a section there where just click "delete my data." It confirms that they want to delete their data, and it's deleted automatically.

Senator HAWLEY. Is that true? Let's take a look. Let's take a look.

Mr. SELSAVAGE. Okay.

Senator HAWLEY. When they go onto your page, they get an opportunity. It says "permanently delete the data." So they click the button that says "permanently delete the data," and then they get a notification that says "Your account is no longer accessible." If they can't access their account anymore, how do they know their data has been deleted?

[Poster is displayed.]

Mr. SELSAVAGE. Because we send them a notification that their information has been deleted.

Senator HAWLEY. You send it once. And how long does that take?

Mr. SELSAVAGE. You know, our policies State that, you know, we will delete their data within 30 days, and in most cases, we—it is automatic and happens much more quickly.

Senator HAWLEY. And when you deleted it, it is deleted, deleted. It is gone forever?

Mr. SELSAVAGE. All the genetic data is deleted forever, and—yes.

Senator HAWLEY. Really? Because that is not what your privacy statement says in the fine print. Let's read it. What your statement says is "We retain personal information for as long as necessary to provide the services and fulfill the transactions you have requested to comply with our legal obligations, resolve disputes, enforce agreements," et cetera, et cetera. And then it goes on, "23andMe and/or our contracted genotyping laboratory will retain your genetic information even if you choose to delete your account."

Mr. SELSAVAGE. Senator, you know, 23andMe, it does not retain any genetic information regarding the consumer once they delete their account. We do——

Senator HAWLEY. It says right here that you will retain genetic information, including date of birth and sex, even if you choose to

delete your account. This is your privacy policy. I am just quoting from it.

Mr. SELSAVAGE. I'm—Senator, you know, to the best of my knowledge, we do not maintain any genetic information.

Senator HAWLEY. It says, "Even if you choose to delete your account, we will retain." "We will retain your genetic information, date of birth and sex, even if you choose to delete your account."

Mr. SELSAVAGE. There is some information that we do retain——

Senator HAWLEY. Aha.

Mr. SELSAVAGE [continuing]. But not related to the genetic information.

Senator HAWLEY. Right.

Mr. SELSAVAGE. But that—you know, such as name, email address——

Senator HAWLEY. Oh.

Mr. SELSAVAGE [continuing]. And other——

Senator HAWLEY. Ah. So even if—ah. Even if you delete the account, you retain their name, you retain their email address, you retain their date of birth, you retain their sex, and you retain their genetic information even if they choose to delete your account. So in other words—don't talk to your suit behind you, talk to me. He is not testifying, you are.

You do not allow consumers actually to delete permanently their data. And when you said a minute ago to Senator Moody, at all times consumers have complete control of their data, that is just not true, is it? By the terms of your own agreement, that just is not true.

Mr. SELSAVAGE. Senator, with all due respect, all of the genetic data is deleted. We are only maintaining——

Senator HAWLEY. With all due respect, what you are telling me is in direct contravention to what your own policy states. "Even if you choose to delete your account." In fact, what you do is you allow your consumers to delete their account settings, but their data isn't deleted. You still have it. The laboratory still has it. You have their name, you have their date of birth, you have their sex, and now you are going to sell it.

Here is my point. It is a pattern. Your consumers actually aren't in control of anything. You are. You control their data. You control their genetic information. Now you are about to sell it. You promise them we won't ever sell it without your consent, but you are doing it. You promise them we will allow you to delete it, but you don't. In fact, you have lied to them, have you not?

Mr. SELSAVAGE. Senator, we have not. We—I assure you that we are deleting all of our customers who have requested——

Senator HAWLEY. No, you are not. You are not because your policies say they are not, and you are not deleting it because if you were, your company wouldn't be worth $300 million.

No, don't read from what your guy behind you is shoveling talking points to you now. I don't want your talking points. I have read your policies. I have seen what they are, and I tell you what, it is amazing to me you are not getting your socks sued off by your customers. I hope they will. I hope they will rush to the courthouse, even as we are here today, to sue you into oblivion for lying to

them and taking their most personal, identifiable information and selling it for a profit and lying to them and to the American public.

Quite frankly, Mr. Selsavage, what you are doing here has all kinds of implications, national security implications, all of it, but nothing is worse than taking the personal, identifiable information of American consumers and keeping it and lying to them about it while you make a huge profit off of it. It is unbelievable to me. It is absolutely unbelievable.

This concludes our hearing. I want to thank each of the witnesses for taking the time to share your experience, your expertise, and your perspectives.

Written questions can be submitted for the record until Wednesday, June 18, at 5 p.m. I will ask the witnesses to answer and return questions to the Committee within 2 weeks.

The hearing is adjourned.

[Whereupon, at 11:58 a.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

Testimony of I. Glenn Cohen

Deputy Dean and James A. Attwood and Leslie Williams Professor of Law, Harvard Law School

Before the

United States Senate

Committee on the Judiciary

23 and You: The Privacy and National Security Implications of the 23andMe Bankruptcy

June 11, 2025

Chairman Grassley, Ranking Member Durbin, and other distinguished members of the Judiciary Committee, my name is I. Glenn Cohen, and I am a Deputy Dean and the James A. Attwood and Leslie Williams Professor of Law, Harvard Law School, and the Faculty Director, Petrie-Flom Center for Health Law Policy, Biotechnology & Bioethics. My research focuses on legal and ethical issues in medicine and the biosciences, including extensive work on genetics and privacy. Thank you for the opportunity to testify before you today about the need to protect genetic data, our existing privacy laws, and the 23andMe bankruptcy.

I want to focus on four main points: (1) Why genetic data is sensitive data and why protecting its privacy is paramount; (2) How the 23andMe bankruptcy highlights the need for legislative action; (3) Why existing federal law protections have significant gaps in protecting genetic privacy; and finally (4) to provide an analysis of some models for possible legislative action.

I. Why Genetic Data is Sensitive Data and Why Protecting Its Privacy is Paramount

Genetic information has some distinct aspects that jointly distinguish it from many other kinds of personal data in ways that are important for privacy. First, it is immutable in that one cannot change one's genetics in the relevant sense. That means that if someone gains access to your genetic sequencing information, that information is forever associated with you, and there is nothing you can do to change that. Second, and relatedly, genetic information is inherently identifiable. While we share the vast majority of our DNA with other human beings, the small amount of genetic variability in my versus your genetic information is enough to directly identify me.[1] Third, access to one's genetic information reveals information not just about oneself but

[1] Luca Bonomi, Yingxiang Huang & Lucila Ohno-Machado, *Privacy Challenges and Research Opportunities for Genomic Data Sharing*, 52 NAT. GENET. 646, 646 (2020).

one's "blood relatives" because of their shared genetic inheritance.[2] Thus, participation in genetic testing like the kind offered by 23andMe exposes not only the customer's genetic information but that of many people related to him or her who never consented. Fourth, many health conditions have significant genetic components such that knowing about someone's genes may tell one a lot about their health.

I am sometimes asked: "Imagine someone had robust access to my genetic information, in concrete terms, what should I worry about?" Here is a non-exhaustive list of answers:

Health Information: Our genetic information can be revealing about our health state and susceptibilities, such as our risk and prognosis for breast cancer, Alzheimer's disease, or many other health conditions.[3]

Identification: Even with an otherwise deidentified genetic sample, researchers have shown the possibility of reidentifying a person from their genetic information using publicly available databases and indeed some have suggested that "whole-genome data may be able to correctly predict physical features, such as eye, hair and skin color, and facial and vocal characteristics."[4]

Discrimination: While, as I will discuss below, current federal law largely protects against employment and health insurance discrimination on the basis of genetic information, it has important gaps in terms of protecting individuals from discrimination by other entities such as in life, disability, and long-term care insurance.

Forensic Uses: A central database, known as the Combined DNA Index System ("CODIS"), allows all U.S. states, the District of Columbia, and several federal agencies to collect, store, and share genetic information for law enforcement uses. Theis includes DNA collected not only from those convicted of felonies, but in many instances, those convicted of misdemeanors, and even those who are arrested but not convicted of any crime.[5] These databases can be used not just to match genetic material collected at a crime scene to an individual but also to identify relatives of that individual who are in the database and impose surveillance on that relative and their family members and/or confront the relative for information. The issues are even more pronounced with the databases of companies like 23andMe that collect much more robust genetic information and can reveal a second, third, or more distant cousin and define the relationship of a person to the genetic sample collected at a crime scene.[6] As a result, many of us can, in a real sense end up in a "DNA dragnet," merely because of genetic relatedness to someone present at a crime scene.

---

[2] *Id.*; Natalie Ram, *Investigative Genetic Genealogy and the Problem of Familial Forensic Identification*, *in* CONSUMER GENETIC TECHNOLOGIES: ETHICAL AND LEGAL CONSIDERATIONS 215 (I. Glenn Cohen, Nita Farahany, Henry T. Greely & Carmel Shachar, eds.) (Cambridge Univ. Press 2021).
[3] Bonomi et al, *supra* note 1, at 646.
[4] Bonomi et al., *supra* note 1, at 646.
[5] Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1382-84 (2019).
[6] *Id.* at 1377-1378.

Misattributed Paternity and Upending Families: In the U.S., it is not standard to conduct a paternity test for children when they are born. A not insignificant portion of the U.S. public would be surprised to find out that their father is not, genetically speaking, who they thought he was. Whether it is a result of adoption, infidelity, embryo mix-ups as part of In Vitro Fertilization, or in some of the darkest cases, sexual assault, knowing someone's genetic information may reveal that their understanding of their family is, genetically speaking, fictitious.[7]

National Security: While others testifying have more expertise in the national security risks, it is notable that in 2019 the Pentagon warned members of the military against using direct-to-consumer genetic tests. A memo from Joseph D. Kernan, the Under Secretary of Defense for Intelligence, and James N. Stewart, the Assistant Secretary of Defense for Manpower and Reserve Affairs, Performing the Duties of the Under Secretary of Defense for Personnel and Readiness, cautioned that "[e]xposing sensitive genetic information to outside parties poses personal and operational risks to service members," that "[t]hese DTC (Direct to Consumer) genetic tests are largely unregulated and could expose personal and genetic information, and potentially create unintended security consequences and increased risk to the joint force and mission," and that "there is increased concern in the scientific community 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."[8]

These are just some of the prominent current known risks. As our knowledge about the human genome increases, many portions of the genetic code that were once thought of as "junk" (in the sense of non-revealing) regions will be recognized as predictive. Moreover, especially when combined with artificial intelligence, we are likely to see more use of genetic information in the future to try to learn about or predict future health conditions of individuals. Genome-wide association studies ("GWASs") use data from biobanks to try to identify correlations between genes and phenotypes (the observed characteristics of an organism) and enable the creation of polygenic risk scores that allow one to sum the effect sizes of all the variants from an individual's genome by using an index derived from population-level studies, that is to aggregate the contributions of multiple genomic loci (with varying effect sizes) to the disease/trait of interest.[9] These scores, some of which have been created using 23andMe data, have been developed not just to predict diseases like breast cancer, but also to try to predict risk tolerance, educational attainment, and other behavioral traits.[10] The value of many of these predictive

---

[7] Kif Augustine Adams, *Generational Failures of Law and Ethics: Rape, Mormon Orthodoxy, and the Revelatory Power of Ancestry DNA*, *in* CONSUMER GENETIC TECHNOLOGIES: ETHICAL AND LEGAL CONSIDERATIONS 273 (I. Glenn Cohen, Nita Farahany, Henry T. Greely & Carmel Shachar, eds.) (Cambridge Univ. Press 2021).
[8] Luis Martinez, *Pentagon Warns Military Not to Use Consumer DNA Kits*, ABC News, Dec 24, 2019, https://abcnews.go.com/Politics/pentagon-warns-military-consumer-dna-test-kits/story?id=67904544
[9] Jin K. Park & I. Glenn Cohen, *The Regulation of Polygenic Risk Scores*, 38 HARV. J. L. & TECH 377, 380-81 (2024).
[10] Shawneequa Caller & Anya E.R. Prince, *The Legal Uncertainties of Sociogenomic Polygenic Scores*, 38 HARV. J. L. & TECH 554, 557-560 (2024).

scores is at the moment quite uncertain, but whatever their quality, one can easily imagine a future where our genetic information is used to try to predict much more about us and our role in society in a way that many might find worrying.

II. How the 23andMe Bankruptcy Highlights the Need for Legislative Action

Since 2006, through its direct-to-consumer genetic tests, 23andMe has amassed a vast database that includes the genetic and personal information of more than 15 million consumers.[11] It is in the midst of selling itself on a fast track in a recently-filed federal bankruptcy case with Regeneron Pharmaceuticals, Inc and TTAM research Institute as leading bidders. While the genetic data controlled by 23andMe is extremely sensitive, its data set -- which would be subject to sale as part of the bankruptcy -- also contains many other forms of personal data including biometric information to verify customers' identity, sample information (including saliva samples and laboratory values), self-reported information related to health, family history, behavior, and registration information (such as name, address, and credit card information), as well as user content (including messages sent via 23andMe's services).[12] The company experienced a significant cybersecurity breach in 2023 that exposed the data of its customers, showing the difficulty in keeping this data secure against cyberattacks.[13]

As I discuss below, while there are some federal and state laws that protect the data of 23andMe's current consumers in bankruptcy, the main privacy protection for its customers is actually a promise that the company has made in its privacy statement. That statement provides customers certain rights, such as the right to opt out of the storage of their saliva samples and the right to request the deletion of their account. It also indicates that 23andMe does not share personal information (i.e., individual-level information, such as information on diseases or genotypes, or deidentified information) voluntarily with insurance companies, employers, or public databases or with law enforcement agencies without a valid subpoena, search warrant, or court order, although the company does share personal information with its service providers and contractors for some purposes.[14]

However, on a closer read, the privacy statement provides less protection than it initially appears and thus highlights the problem with leaving decisions about the privacy protection of genetic material to individual company policies and consumer consent.

---

[11] Sara Gerke, Melissa B. Jacoby & I. Glenn Cohen, *Bankruptcy, Genetic Information, and Privacy—Selling Personal Information*, 392 NEW ENG. J. MED. 937 (2025), https://www.nejm.org/doi/abs/10.1056/NEJMp2415835; *An Open Letter to 23andMe Customers*, 23ANDME, https://blog.23andme.com/articles/open-letter (last visited June 7, 2025).

[12] Sara Gerke, Melissa B. Jacoby & I. Glenn Cohen, *23andMe's Bankruptcy Raises Concerns about Privacy in the Era of Big Data*, 389 BMJ r1017 (2025), https://www.bmj.com/content/389/bmj.r1071; *Privacy Statement*, 23ANDME, https://www.23andme.com/legal/privacy/full-version/ (last visited June 7, 2025).

[13] Gerke et al, *supra* note 11, at 938; *Privacy Statement*, 23ANDME, *supra* note 12.

[14] Gerke et al, *supra* note 11, at 938; *Privacy Statement*, 23ANDME, *supra* note 12.

First, it bears emphasizing that the assumption that individuals carefully read and fully understand the privacy policy or terms of service blinks reality. As one set of authors wrote regarding terms of service more generally, "only 1 in 1000 visit terms of service; that number drops to 1 in 10 000 if getting there requires 2 clicks. The median reading time is 29 seconds."[15]

Second, 23andMe reserves the right to unilaterally alter these terms. It indicates: "We may make changes to this Privacy Statement from time to time. We'll let you know about those changes here or by reaching out to you via email or some other contact method, such as through in-app notification, or on another website page or feature."[16] Such changes could be radical and vitiate the promises customers relied on, for example, more readily sharing information with law enforcement or insurers than under the company's current policy. Moreover, 23andMe explicitly reserves the right to transfer customers' personal information in the event of a sale of the company or bankruptcy, and the company explicitly notes that the customer's personal information may be "accessed, sold or transferred as part of that transaction."[17]

The company has announced that as part of the bankruptcy process it "required anyone bidding for 23andMe to agree to comply with our privacy policies and all applicable privacy laws."[18] That is all well and good, but even if that becomes a condition of the sale nothing prohibits Regeneron, TTAM, or another buyer of the data from altering that privacy policy after a change in ownership of the data, just as there was nothing to stop 23andMe from doing so.[19] It is also unclear to me under the company's existing privacy policy how the stored customer saliva samples will be handled as part of the bankruptcy, and this may raise an additional problem for customers' privacy.

Trust is all about a relationship. Customers who chose 23andMe entered into a particular kind of relationship with a particular kind of company: they shared their genetic and other personal information, recognizing there was some privacy risk, to obtain potential ancestry and health-related insights. Some 23andMe consumers also opted in to research use, to help enable research and the development of potential new drugs or other therapeutics. Upon bankruptcy or sale of assets, consumers may end up in a relationship with a very different kind of company with goals they may not support and policies that have changed while they were not looking.

To some extent, bankruptcy offers an extra layer of privacy protection for the transfer of genetic information as compared to other methods of sale or acquisition. Under federal bankruptcy law in some instances a consumer privacy ombudsperson may be appointed to investigate the sale

---

[15] Anya E.R. Prince & Kayte Spector-Bagdady, *Protecting Privacy When Genetic Databases Are Commercialized*, 333 JAMA 665 (2025) (citing Yannis Bakos, Florencia Marotta-Wurgler, and David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J.L. STUDIES 1 (2014)).
[16] *Other Things to Know About Privacy*, 23ANDME, https://www.23andme.com/legal/privacy/#other-things-to-know (last visited June 7, 2025).
[17] Gerke et al, *supra* note 11, at 938; *Privacy Statement*, 23ANDME, *supra* note 12.
[18] *An Open Letter to 23andMe Customers*, *supra* note 11.
[19] Gerke et al, *supra* note 11, at 938.

and determine compliance with the bankrupt company's privacy statement and applicable non-bankruptcy law.[20] In this case, a well-regarded privacy law expert has been appointed to this role. That may not be the case for all forms of sale of genetic data, which underscores the need for more protection. Privacy statements and customer acquiescence have a role to play, but private ordering solutions can only go so far to deal with the concerns. More structural solutions through the legislative process are also needed.

III. Existing Federal Law Protections Have Significant Gaps in Protecting Genetic Privacy

There are a few important pieces of federal law that one might think would protect genetic privacy. Unfortunately, they either do not apply in this kind of case or only partially solve the problems identified.

First, given the amount of health-related information 23andMe collects and analyses, one might think the protections of our main federal health privacy law, the Health Insurance Portability and Accountability Act (HIPAA), would be important.[21] Unfortunately, as a direct-to-consumer genetic testing company, 23andMe is not considered a covered entity or a business associate of such an entity under the statute and therefore is not covered under HIPAA's requirements. In lay terms, individuals interact with the company as consumers, not as patients, and thus it escapes this regulatory regime.

Second, the Genetic Information Nondiscrimination Act (GINA),[22] would seem to be very helpful in assuaging fears related to genetic privacy. The Act prohibits discrimination based on an individual's genetic information by covered employers and health insurers. Congress passed GINA nearly unanimously, and it was signed into law by President George W. Bush in 2008. The statute's goal was to address fears about genetic discrimination, allowing Americans to feel comfortable participating in research and to benefit from genetic medicine.

The statute has provided valuable protection, but that protection is incomplete. GINA does not protect against genetic discrimination for life, disability, and long-term care insurance, nor does it apply to some small businesses, military employees, and some other groups subject to exceptions.[23] Many of our peer countries have gone further either through legislation or compacts with the insurance industry: For example, France strictly limits the use of genetic testing to medical or scientific reasons, while countries such as Australia, Switzerland, and the

---

[20] Gerke et al, *supra* note 11, at 938.
[21] 42 U.S.C. § 1320d et seq.; 45 C.F.R. Parts 160 and 164.
[22] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881.
[23] Jean-Christophe Bélisle-Pipon, Effy Vayena, Robert C. Green & I. Glenn Cohen, *Genetic Testing, Insurance Discrimination and Medical Research: What the United States Can Learn from Peer Countries*, 25 NAT. MED. 1198, 1199 (2019).

United Kingdom do not allow the consideration of genetic information in life and disability insurance under a certain financial limit.[24]

Importantly, GINA also excludes protection from discrimination on the basis of conditions that have already *manifested* in the individual.[25] While in some cases the Americans with Disabilities Act (ADA), as amended, will protect such individuals, there may be cases that fall within the gap between GINA and the ADA.

Finally, it is worth emphasizing that freedom from discrimination is just one of the concerns that explain why genetic privacy is so important. Thus, even where GINA succeeds, it may leave many of the concerns unaddressed.

IV. Analysis of Models for Possible Legislative Action

As I hope I have made clear, while the sale of genetic information as part of a bankruptcy proceeding is what has led us to this hearing today, it just shines a light on a much larger set of issues with genetic privacy in the U.S.

It is also important to recognize that direct-to-consumer genetic testing companies like 23andMe have provided a service that many customers have valued. Moreover, as the federal government's commitment to the NIH All of Us program demonstrates, large genetic databases are crucial to building the next generation of therapeutics and improving our understanding of disease. 23andMe should be appropriately recognized for its own contributions to such research.

The question is: Are there good legislative actions that could reduce some of the genetic privacy risks without unduly hampering research and innovation? It is useful to think about intervening at different scales of the problem.

Comprehensive Privacy Legislation at the Federal Level: At the most ambitious level, some jurisdictions have attempted more comprehensive data privacy regulation that have specific rules for genetic information. The EU General Data Protection Regulation (GDPR) applies to all personal data and provides heightened protection for genetic and health data, which in essence by default bans processing (including collection, use, or disclosure) of genetic data and data concerning health unless an exception applies, such as with a customer's explicit consent under specific conditions.[26] Some states have also tried to implement comprehensive privacy legislation. Whether this is a feasible approach for the U.S. is a much bigger conversation.

Genetic Privacy: One level down is to focus only on genetic privacy. Here, some of the foreign antidiscrimination laws mentioned above might suggest amendments to GINA that would extend protection to life, disability, and long-term care insurance, perhaps only for policies below a

---

[24] *Id.*; Anya E.R. Prince, *Political Economy, Stakeholder Voices, and Saliency: Lessons from International Policies Regulating Insurer Use of Genetic Information*, 3 J. L. & BIOSCI. 461 (2018).
[25] Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L. J. 544 (2019).
[26] Gerke et al, *supra* note 12, at r1071.

certain limit. Indeed, we have a good model at the state level. In 2020, Florida became the first U.S. state to ban insurers from discriminating on the basis of genetic information in areas not covered by GINA - life, long-term care, and disability insurance.[27] While federalism has many virtues, when it comes to freedom from discrimination in insurance it is less clear why those purchasing policies in some states should have more protections than those in other states. It would be worthwhile to consider extending similar protection at the federal level.

A different approach is to consider extending some of the existing HIPAA law to direct-to-consumer genetic testing companies and biotechnology or pharmaceutical companies or others buying or collecting this kind of data, treating them, where appropriate, as covered entities and regulating them more like health care systems.

Another approach is provided by the Genetic Information Privacy Act, a model law developed by 23andMe and Ancestry that has been adopted in several U.S. states.[28] The model Act requires companies to, among other things:

> provide clear notices of their privacy practices that are written in plain language, and must obtain express consent from consumers for numerous practices, including the collection, sharing, and continued storage of their genomic data, as well as other activities, such as marketing. Consumers must be able to revoke their consent and have their biospecimens destroyed. Companies also are required to establish strong security protections to minimize risk of unintended disclosure.[29]

While the model Act contains some valuable protections, some have criticized it as being too permissive in terms of permitting sharing genetic information with law enforcement and that its reliance on a notice-and-consent model is unrealistic given that so few individuals meaningfully engage with privacy policies.[30] It also has a more limited scope, applying by its terms only to a company that "(a) offers consumer genetic testing products or services directly to consumers; or (b) collects, uses, or analyzes genetic data that a consumer provides to the entity."

Regulating Bankruptcy, Sale, and Transfer of Assets of Direct-to-Consumer Genetic Testing Companies: Finally, legislative action could focus on something akin to the facts of this particular case -- how to handle the transfer of assets in bankruptcy or other sale of a company like 23andMe.

---

[27] A.C.F. Lewis, R.C. Green, A.E.R. Prince, *Long-awaited Progress in Addressing Genetic Discrimination in the United States*, 23 GENET. MED. 429 (2021).
[28] *See, e.g.*, Utah S.B. 227 Genetic Information Privacy Act (2021), https://le.utah.gov/~2021/bills/static/SB0227.html; Anya E. R. Prince, *The Genetic Information Privacy Act: Drawbacks and Limitations*, 330 JAMA 2049 (2023).
[29] *Id.*
[30] *Id.*

One such bill, the Genomic Data Protection Act, S. 5433, sponsored by Senators Cassidy and Peters, has been introduced in the Senate.[31] The bill would with limited exceptions regarding law enforcement and other laws), among other things: (1) Require direct-to-consumer companies to "provide an effective mechanism" to consumers to delete an account, genetic data, or request destruction of biological samples; (2) Upon purchase or other acquisition of such a company require that adequate notice be provided to consumers and reminders of their rights to deletion/destruction of data/biospecimens and confirmation of the appropriate action. The Bill also specifies that a "violation of this section or a regulation promulgated thereunder shall be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act."

Another recent Bill introduced by members of this committee, Chairman Grassley, and Senators Cornyn and Klobuchar, the Don't Sell My DNA Act,[32] would laudably clarify the definition of "personally identifiable information" in the Bankruptcy Code to include genetic information as covered in GINA. It would also importantly require that "no use, sale, or lease shall be approved if the personally identifiable information consists, in whole or in part, of genetic information unless all affected persons, including non-parties, have affirmatively consented in writing to such use, sale, or lease after the commencement of the case," and that notice be given to all affected persons. Finally, it would require the trustee or debtor in possession of the covered genetic information to permanently delete any data not subject to the sale or lease.

I think both bills would make helpful steps to improve genetic privacy, but I particularly endorse the model of strong affirmative consent in the Don't Sell My DNA Act and the deletion of data that is not subject to the sale or lease. It may be worthwhile to expand that Act's coverage to directly address the saliva samples or other biospecimens held by companies like 23andMe. There are, of course, limits to relying on action by consumers themselves to protect genetic privacy, but I think the approach of this bill would go a long way to ameliorating the situation. At the same time, this may be a good opportunity to consider supplementing this approach with other substantive protections and to consider issues of genetic privacy that go beyond the bankruptcy context.

V. Conclusion

The 23andMe bankruptcy has drawn significant attention to the current state of genetic privacy in the U.S., and just how many millions of Americans are exposed. While in this instance the issue has emerged in the context of a company going bankrupt, there are many other ways in which genetic privacy is at risk. Americans deserve more protection for their genetic privacy, and there are some good models for possible legislation in this space for this Committee to consider. Chairman Grassley, Ranking Member Durbin, Members of the Committee, I am appreciative of

---

[31] S.5433. https://www.congress.gov/bill/118th-congress/senate-bill/5433/text/is
[32] https://www.grassley.senate.gov/imo/media/doc/dont_sell_my_dna_act.pdf

your focus on this important issue, and I thank you for the opportunity to testify before you today. I look forward to answering your questions.

WRITTEN TESTIMONY OF

Brook Gotberg
Professor of Law
Brigham Young University

Presented before the U.S. Senate Committee on the Judiciary

Full Committee Hearing: *23 and You: The Privacy and National Security Implications of the 23andMe Bankruptcy*

June 10, 2025

Chairman Grassley, Ranking Member Durbin, and distinguished Members of the Committee:

Thank you for the opportunity to be here. I hope to provide some necessary context to the conversation on how best to protect the privacy of consumers when their personal data is held by corporations in financial distress. The most important concept I wish to convey is that the protection of personal consumer data is not fundamentally nor primarily an issue of bankruptcy law. I encourage the Committee to forego legislation that would introduce new restrictions specific to bankruptcy proceedings and instead pursue methods of protecting personal consumer data that will be broadly applicable. Bankruptcy-specific privacy legislation will not adequately protect consumers' privacy interests and will likely lead to destructive strategic machinations that undermine bankruptcy's core purposes.

The recent bankruptcy of 23andMe Holding Co. has raised awareness of privacy concerns associated with the sale of personal consumer data, but those same privacy concerns also exist when data is sold by non-bankrupt companies. Restrictions on the sale and general use of personal consumer data are typically established by private contractual agreements. Those agreements may be violated whether a sale occurs inside or outside bankruptcy proceedings, harming affected consumers equally in either scenario. Current bankruptcy law provides some oversight that can prevent the worst privacy policy abuses in a bankruptcy sale, but it does not prohibit the sale from taking place. Placing a prohibition on bankruptcy sales would simply push them outside bankruptcy proceedings, where there are fewer protections. The best policy would make any restrictions on the sale of personal consumer data universally applicable.

The sale of valuable assets, including personal consumer data, is frequently associated with severe financial distress; healthy companies are less likely to sell off substantial assets, particularly if doing so raises questions of compliance with their privacy policies. When insolvent companies sell personal consumer data, consumers are limited in their ability to enforce the terms of the privacy policy, whether or not the company is in bankruptcy proceedings. The liquidation of a company ensures that it cannot fulfill the terms of its privacy policy going forward: it makes no difference whether liquidation is accomplished under federal

bankruptcy law or pursuant to state law. Even if an insolvent company continues as a going concern, consumers' rights to enforce their agreements must compete with other claims against the company. An insolvent company cannot satisfy all the claims raised against it.

Bankruptcy provides important advantages when a company is insolvent. The primary goal of bankruptcy is to limit the losses caused by insolvency. It accomplishes this through a coordinated, systematic approach to distribution of assets. This approach minimizes destruction of the debtor's available assets and the costs of recovering those assets, thereby maximizing returns to creditors. The advantages of a bankruptcy system were recognized by the drafters of the Constitution[1] and our nation's bankruptcy laws have subsequently helped to shape the national economy in positive ways.

When a company violates any kind of agreement, including a privacy policy, that violation gives rise to a "claim" in bankruptcy proceedings.[2] Claims include pre-bankruptcy violations but may also arise post-filing.[3] The most common bankruptcy claims are simple rights to payment arising from a deliberate extension of credit, but a claim may also be a right arising from the violation of an agreement. When a bankrupt company has personal consumer data that may be profitably sold in violation of a privacy policy agreement, the interests of consumers in preventing the sale will directly conflict with the interests of other creditors in repayment from the debtor's assets. In other words, selling the data can maximize the return for creditors, but only if consumers' privacy interests are sacrificed. Both groups are considered to have a claim against the bankrupt company, the one for fulfillment of the promises made under the privacy policy, and the other for promises of payment. Under the law, both groups' claims have equal priority.[4]

Since 2005, the question of whether to permit the sale of personal consumer data in violation of a privacy policy is weighed in bankruptcy court by the bankruptcy judge, frequently with the assistance of a consumer privacy ombudsman (CPO). However, the interests of consumers in preserving their rights under a privacy policy are not otherwise afforded priority under the law.[5] Appointing a CPO in these cases is considered necessary in part because it is challenging for a court to interpret the relevant parameters of privacy policies to determine if there is a violation, and if there is, to monetize the cost of privacy losses caused by that violation. The role of the CPO is to assist the court in weighing the costs and benefits of the sale and to explore potential alternatives that would mitigate privacy losses. In most cases, the CPO recommends the court approve the proposed sale of personal consumer data, even if it violates an applicable privacy policy.[6]

---

[1] U.S. CONSTITUTION, Art. I, sec. 8, cl. 4.
[2] *See* 11 U.S.C. § 101(5) (defining "claim" to include any right to payment or equitable remedy for breach).
[3] For example, a debtor may reject an executory contract, giving rise to a claim for damages as if the debtor had breached the contract just prior to the bankruptcy filing. *See* 11 U.S.C. § 365(g).
[4] Some types of claims have priority over others. Most notably, claims that are secured by specific collateral are paid from that collateral ahead of all other claims. *See* 11 U.S.C § 506(a). Priority unsecured claims include domestic support obligations, employee wages, and taxes. *See generally* 11 U.S.C. § 507.
[5] *See generally* 11 U.S.C. § 332. This provision was added to the Bankruptcy Code as part of the Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA).
[6] *See* Christopher G. Bradley, *Privacy for Sale: The Law of Transactions in Consumers' Private Data*, 40 YALE J. ON REG. 127, 135 (2023).

Congress could pass a law that would prohibit the sale of personal consumer data in bankruptcy. Such a prohibition would create a scenario in which distressed companies who cannot profitably use their data could not invoke the protections of the bankruptcy statute, including the automatic stay and an approving order from the bankruptcy judge, to sell those assets. Bankruptcy protections are intended to facilitate the sale of assets, so the sale will obtain the maximum price possible. If sale in bankruptcy is impossible, distressed companies in need of cash will probably just sell personal consumer data outside bankruptcy proceedings, where there is less transparency and very little oversight. The sale will likely result in a lower price and therefore a lower recovery for creditors, but it can still take place absent any legal prohibition outside of bankruptcy.

A sale of personal consumer data conducted outside bankruptcy could proceed even if the sale violated an applicable privacy policy. Consumers would then find themselves in the same position as they would be in if the sale had occurred in bankruptcy, except without bankruptcy's characteristic structure, transparency, and oversight. The primary remedy for consumers when a privacy policy is violated is a claim for breach against the selling company. While the damages associated with such a breach might deter a solvent company from violating its privacy policies, an insolvent company cannot fulfill all its obligations and so is likely to breach whichever agreements are least costly. In many cases, given the difficulty of enforcing privacy policies for the average consumer, the least costly option is to conduct the sale and incur whatever damages may be associated. Unless the breach catches the attention of government enforcement, such as the Federal Trade Commission or a state attorney general, a sale in violation of the applicable privacy policy may be accomplished without repercussion.[7]

Outside bankruptcy proceedings, those with claims against an insolvent debtor find themselves in competition for satisfaction, because every dollar paid to one creditor is a dollar less available for the others. This competition among creditors is costly and socially wasteful; avoiding the costs of zero-sum competition among creditors is a primary reason for bankruptcy law. In bankruptcy, all claims against the debtor are resolved through an orderly distribution of assets, removing the opportunity for competition. Whether claims arise before or after a bankruptcy filing, they are treated the same. Consumers have the same rights whether a company violates its privacy policy through a sale before or after its bankruptcy filing. The primary difference is that bankruptcy proceedings allow the sale to obtain the best price possible with the least invasion of consumer privacy possible, thus maximizing the assets available to compensate consumers for the sale of their data.

I recommend against any proposal that would create a bankruptcy-specific limitation on the sale of personal consumer data. Such a prohibition would merely encourage the sale of data outside bankruptcy proceedings. Bankruptcy law is frequently the best means of managing an insolvent company's assets and resolving its liabilities. When an insolvent company holds personal consumer data, bankruptcy provides the best chance to dispose of that data in a way that is in the best interests of all parties. Bankruptcy sales are preferable to disposition outside bankruptcy,

---

[7] *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016).

because they allow for greater oversight, transparency, and the maximization of return for creditors.

If Congress determines that regulation is required, it should instead impose restrictions on the sale of personal consumer data more generally. It is my recommendation that the law provide greater clarification to consumers of their rights to privacy, facilitating enforcement of those rights both inside and outside bankruptcy proceedings. Clarification could be achieved by creating a set of regulations or standardized expectations for the sale and other use of personal consumer data, including a statutory penalty for violations. This would prove beneficial to all consumers by providing them with the tools they need to meaningfully hold companies accountable to the terms of their privacy policies. It would also lead to greater efficiencies when personal consumer data is sold in bankruptcy proceedings by establishing a set value for the cost of privacy loss. Privacy concerns, thus monetized, could then be more consistently balanced against the interests of other creditors in the sale. This would further the bankruptcy goal of minimizing the harm caused by a debtor's insolvency.

I. Private Data as a Transferable Asset

Current federal law imposes relatively few restrictions on a company's ability to gather, aggregate, anonymize, and sell consumer data. Some notable exceptions to this statement include protection of individuals' medical records (HIPAA)[8] and the data provided by children under the age of 13 (COPPA).[9] Federal law also provides a general backstop of consumer protection, but the application of these legal generalities to any particular scenario is often uncertain at best. Most legal challenges result in settlement, which means that parties lack the certainty of judicial precedent.[10] State-specific privacy laws may apply, but these frequently contribute to the confusion over what is or is not permissible by creating inconsistent and potentially conflicting regimes for companies operating across state lines.

Thus, for the most part, consumer data gathered by a company may be transferred, sold, and leveraged like any other form of corporate property. This freedom permits the holders of the data to capitalize on its value, creating economic wealth. It is a matter of public policy, beyond the scope of my comments, whether such free exchange of consumers' personal information is ultimately a social good.

The relevant legal status of consumer data, including whether it can be bought or sold, is determined by law that applies equally inside and outside bankruptcy proceedings. If property would be available to satisfy a creditor's claims under state or federal law, it is available to satisfy creditors under bankruptcy law. On the other hand, property that is heavily regulated by state and federal law, such as an attorney's license to practice law, a doctor's license to practice

---

[8] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191; 45 C.F.R. §§ 160-164 (2013).
[9] The Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505; 16 C.F.R. Part 312.
[10] *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

medicine, or a liquor license, is often not considered an asset and is therefore nontransferable in bankruptcy.[11]

Congress could impose additional restrictions on the use and sale of personal consumer data generally, as it has with HIPAA and COPPA. Those restrictions would be applicable in any bankruptcy proceeding in which the regulated data was implicated.[12] Although concerns regarding personal consumer data frequently arise in bankruptcy cases, Congress should not create bankruptcy-specific restrictions on the sale of personal consumer data. Bankruptcy-specific restrictions would promote strategic workarounds that would not protect consumers but would impose additional costs on creditors in bankruptcy.[13]

II. Contractual Regulation of Personal Consumer Information

Absent a formal legal prohibition on the use of personal consumer information, the exchange of personal consumer data is governed by private contractual agreement between companies and customers. In most cases, consumers provide personal information to companies under a system of "notice and consent": the company provides an explanation of its privacy policy and the consumer agrees to it. Privacy policies are often difficult to understand and may be internally inconsistent.[14] Conventional wisdom is that consumers rarely even read privacy policies before consenting to them.

Privacy policies often afford the company gathering personal consumer data the freedom to sell it in the interest of business continuity. A business continuity provision envisions a scenario in which the original business will be sold, merged, or otherwise transferred to a new buyer, and reserves the right to transfer data along with the rest of the business. Frequently, but not always, the provision may guarantee that the buyer will continue to respect the same privacy terms to which the consumer originally agreed. The privacy policy adopted by 23andMe in June of 2022 is typical. It reads:

> **Commonly owned entities, affiliates and change of ownership**: If we are involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your Personal Information may be accessed, sold or transferred as part of that transaction and this Privacy Statement will apply to your Personal Information as transferred to the new entity. We may also disclose Personal

---

[11] *See, e.g.*, Wade v. State Bar of Arizona (*In re* Wade), 115 B.R. 222, 228 (B.A.P. 9th Cir. 1990) aff'd 948 B.2d 1122 (9th Cir. 1991) (attorney's license is not property); *In re* Circle 10 Rest., LLC, 519 B.R. 95, 129 (Bankr. D. N.J. 2014) (a liquor licenses is a temporary permit or privilege and not property); Ryan v. Lynn, (*In re* Lynn), 18 B.R. 501, 503 (Bankr. D. Conn. 1982) (a license to practice medicine is not property for the purposes of bankruptcy law). Other courts have concluded that a liquor license is property of the bankruptcy estate, and the question is somewhat unsettled. *See, e.g., In re* The Ground Round, Inc., 482 F.3d 15, 17 (1st Cir. 2007).

[12] *See* 11 U.S.C. § 363(b)(1)(B)(ii) (a bankruptcy sale cannot violate applicable nonbankruptcy law).

[13] Consider, for example, the numerous loopholes and workarounds apparently permitted under the current CPO provisions. *See* Christopher G. Bradley, *Privacy Theater in the Bankruptcy Courts*, 74 HASTINGS L.J. 607, 622-30 (2023).

[14] *See* Christopher G. Bradley, *Privacy Policy Indeterminacy*, 56 CONN. L. REV. 407, 411, 424 (2024).

> Information about you to our corporate affiliates to help operate our services and our affiliates' services.[15]

Despite this language, several parties objected to 23andMe's proposal to sell personal consumer data in its bankruptcy filing, alleging that the sale violated the terms of the company's privacy policy, in addition to several state privacy laws.[16]

The legal and factual issues associated with this objection are complex, and unlikely to be finally resolved or even fully litigated in the bankruptcy proceedings.

III. Enforcement of Privacy Policies

The legality of 23andMe's proposed bankruptcy sale is unlikely to be fully litigated because doing so would require an unsupportable dedication of resources to the legal dispute, in a situation where the company is already financially distressed and its creditors unlikely to be repaid in full. However, similar litigation is unlikely to occur even outside bankruptcy proceedings because of the complexity of the legal issues involved and the uncertainty of any recovery for plaintiffs.

Individual consumers are legally entitled to enforce agreements to preserve the privacy of their data. But individuals are unlikely, even in the best of circumstances, to successfully bring a legal claim to defend their rights when a business fails to fulfill the promises made in its privacy policy. For example, a consumer could not prevail in a bid to force a failing company to preserve personal consumer data as envisioned under the privacy policy. A defunct company cannot be held responsible for the safe storage of personal consumer data – if the company fails, there is no one to hold accountable for this obligation. Accordingly, consumers may be harmed even if a company does not sell its personal consumer data, because a failure to maintain adequate safety precautions could subject the data to inadvertent disclosure. Often the harm caused by a violation of the privacy policy is difficult to quantify, and any damages equally difficult to prove. In nearly every imaginable scenario, the cost of filing a lawsuit will be prohibitively expensive for any given individual whose data is implicated in a privacy policy violation, especially when there is no guarantee of success. This is particularly true when the defendant company is financially distressed.

The Federal Trade Commission or state attorneys general are more likely to successfully raise complaints associated with the mismanagement or sale of personal consumer data. They have the advantages of public resources and can represent the interests of a large number of affected consumers. But they face many of the same challenges to establishing a violation of an applicable privacy policy and proving damages.

Current privacy policies are not standardized, but use individualized contractual language from policy to policy. This requires litigants to establish the parameters of each individual policy as a

---

[15] https://www.23andme.com/legal/privacy/full-version/ (last updated March 14, 2025).

[16] *See, e.g.*, Motion for the Appointment of a Consumer Privacy Ombudsman and a Security Examiner Pursuant to 11 U.S.C. Sections 105(a), 332, 363(b)(1) and Federal Rule of Bankruptcy Procedure 6004(G) and Notice of Hearing, Doc. 239, *In re* 23andMeHolding Co., Case No. 25-40976 (Bankr. E.D. Mo. Apr. 15, 2025).

matter of contractual interpretation before a violation can be established. The diversity of language used in privacy policies also virtually assures that consumers, who regularly agree to privacy policies without reading them, have little hope of knowing what each individual privacy policy permits the contracting company to do with the data it gathers. This increases the difficulty of recognizing when a violation has taken place.

One legal approach to these problems, as noted above, is simply to introduce a body of regulation like the area-specific regulations governing certain health data or data on children. Another more flexible method to improve the enforcement of privacy policies both inside and outside bankruptcy might be to establish a standardized set of privacy policies associated with personal consumer data.[17] These privacy policies could cover a range of options, from the most permissive use of personal consumer data permitted under the law to the most restrictive use feasible. For example, Privacy Policy A might mirror the stated policy of Skipity.com, which begins, "[w]e firmly believe that privacy [is] both inconsequential and unimportant to you. . . . If you're one of those tin-foil-hat wearing crazies that actually cares about privacy: stop using our services and get a life."[18] On the other hand, Privacy Policy D might guarantee that all personal consumer data would remain with the company for the duration of the company's existence, never be sold despite any other asset sale or merger, and be destroyed should the company cease to operate.

With relatively few standardized provisions in circulation, individual consumers would be far more likely to recognize and understand the ramifications of a given privacy policy. Standardization would also greatly simplify the enforcement of privacy policies by clarifying their parameters. This clarification would make it easier to recognize when a violation of a privacy policy has occurred.

IV. Bankruptcy Law's Alteration of Nonbankruptcy Rights

Although personal consumer data is sold on a regular basis in standard business transactions, concerns regarding the sale of personal consumer data tend to arise with greater frequency in the bankruptcy context. This may be, in part, a function of the increased public scrutiny afforded to such sales by virtue of the public notices required in bankruptcy. In bankruptcy proceedings, a distressed company must provide notice of its intent to sell personal consumer data. A judge must approve any sale of assets by a bankrupt debtor, commonly through proceedings outlined in Section 363 of the Bankruptcy Code.[19] These are accordingly referred to as "363 sales." Alternatively, a debtor's assets might be sold following approval of a plan of reorganization.

The primary difference between a 363 sale and a plan of reorganization is the involvement of individuals with claims against the debtor, collectively referred to as creditors.[20] In order to

---

[17] I largely echo another scholar's recommendation on this issue. *See* Christopher G. Bradley, *Privacy Policy Indeterminacy*, 56 CONN. L. REV. 407, 430-32 (2024).
[18] *Skipity.com*, *Privacy Policy Terms and Conditions*, INTERNET ARCHIVE: WAYBACK MACHINE (Feb. 13, 2016), https://web.archive.org/web/20160213180839/skipity.com/privacy (cited in Christopher G. Bradley, *Privacy Policy Indeterminacy*, 56 CONN. L. REV. 407, 407 (2024).
[19] 11 U.S.C. § 363.
[20] *See* 11 U.S.C. § 101(10).

approve a plan, all creditors must have the opportunity to vote for or against the proposed plan. A plan of reorganization must be approved by a majority of voting creditors, separated into classes based on the similarity of their legal rights against the debtor.[21] Most of the sales of personal consumer data that attract the concern of the public are 363 sales, in which creditors do not have the opportunity to vote for or against the sale. This is the type of sale at issue in the 23andMe bankruptcy.

The purpose of the 363 sale is to preserve the value of the debtor's assets to the extent possible. A plan of reorganization may take several months to confirm,[22] during which time assets can depreciate in value.[23] A higher sale price ensures a larger recovery for creditors, minimizing the loss they must bear as a consequence of the debtor's insolvency.

Although creditors do not vote in a 363 sale, bankruptcy proceedings do provide the oversight of the bankruptcy judge, who conducts a hearing to consider the sale and may approve or deny it. In 363 sale situations where personal consumer data is implicated, a CPO may also be appointed to assist the bankruptcy judge; there is no CPO when a sale takes place as part of a reorganization plan.[24] The legislative history suggests that the CPO position was created to prevent the sale of personal consumer data in bankruptcy in violation of established privacy policies.[25] Empirical research has indicated that in most cases where a CPO is appointed, the sale of personal consumer data in violation of a privacy policy is nevertheless approved, in nearly every instance at the CPO's recommendation.[26]

The CPO's charge is primarily to provide the judge with information regarding the privacy ramifications of the sale, and to identify potential alternatives that would mitigate privacy losses.[27] The CPO does not typically assign a dollar value to the privacy losses, likely because any attempt to do so would be at best a shot in the dark. The CPO may have very little time – as little as seven days – to conduct the necessary review prior to the hearing on the sale.[28] The expenses of that review are paid out by the bankruptcy estate and accordingly borne by the creditors, creating pressure to keep the review narrow.[29] Although the CPO may provide value to the court in weighing the costs and benefits of permitting the sale, he or she must usually do so in the absence of a final adjudicated determination that the sale violates the relevant privacy policy. Because the CPO increases the costs of the sale and potentially delays its consummation,

---

[21] *See* 11 U.S.C. §§ 1122; 1126; 1129(a)(8).
[22] *See* Foteini Teloni, *Chapter 11 Duration, Pre-Planned Cases, and Refiling Rates: An Empirical Analysis in the Post BAPCPA Era*, 23 ABI L. REV. 571, 582 (2015) (concluding from an empirical study of public companies that the duration of traditional chapter 11 cases after 2005 is 430 days).
[23] The extent to which this occurs may be overstated, but the possibility is undisputed. *See generally* Melissa B. Jacoby & Edward J. Janger, *Ice Cube Bonds: Allocating the Price of Process in Chapter 11 Bankruptcy*, 123 YALE L. J. 862 (2014).
[24] *See* 11 U.S.C. § 332(a).
[25] *See* Congressional Record 107 Cong. 147 (March 5, 2001) (Statement of Orrin Hatch) at S1795.
[26] *See* Christopher G. Bradley, *Privacy Theater in the Bankruptcy Courts*, 74 HASTINGS L. J. 607, 653 (2023) ("nearly every report reflects the [CPO] tinkering with aspects of proposed sales while ultimately letting them proceed").
[27] 11 U.S.C. § 332(b).
[28] *See* 11 U.S.C. § 332(a).
[29] *See* 11 U.S.C. § 330(a)(1).

both the debtor and creditors in bankruptcy proceedings often seek to avoid a CPO appointment, as 23andMe did.[30]

Balancing the interests of consumers in the enforcement of a company's privacy policy against the interests of creditors in recovering from the debtor's assets is an extremely difficult and complex endeavor. It could be simplified by establishing statutory damages in connection with privacy policy violations. The easier it is to assign damages, the easier it would be for a court to weigh the costs of permitting violation of a privacy policy against the benefit to creditors. Congress could assign statutory damages that would make any sale in violation of a privacy policy prohibitively expensive. In that scenario, such sales would be less likely to occur in or out of bankruptcy. The bankruptcy court would not approve such a sale because it would not be in the best interests of creditors.

Conclusion

In summary, I present the following recommendations to the Committee:

- **Apply one rule to every sale of personal consumer data**. Congress should ensure that any restriction is applicable both inside and outside bankruptcy proceedings to maximize the protections afforded to consumers. A prohibition on bankruptcy sales would leave consumers vulnerable to the sale of their data outside bankruptcy, undermining the protections and advantages bankruptcy proceedings are intended to provide.

- **Create a standardized understanding of consumers' rights to data privacy.** Current contractual agreements make it extremely difficult to understand or enforce the provisions of a privacy policy. Better clarity on what consumers might expect can ensure better enforcement of consumers' rights.

- **Establish statutory damages for violations of privacy agreements involving personal consumer data**. Giving all parties a clear understanding of the cost to violating privacy policies will allow them to make more informed decisions on whether and when data can be sold.

Congress may choose to impose legal restrictions on the sale of personal consumer data. These restrictions might include a total prohibition on the sale of some types of data, requirements that companies standardize their privacy policies, or any number of alternative approaches. Whatever approach taken, Congress should avoid creating a bankruptcy-specific rule that might inadvertently undermine the purposes of bankruptcy.

Respectfully submitted,
Brook Gotberg

---

[30] *See* Christopher G. Bradley, *Privacy Theater in the Bankruptcy Courts*, 74 HASTING L. J. 607, 635 (2023).

Brook Gotberg is a Professor of Law at BYU's J. Reuben Clark Law School, specializing in bankruptcy and commercial law. Her scholarship addresses consumer and corporate distress, with a particular emphasis on small- and medium-sized businesses. She presents regularly to academic and professional audiences across the U.S. and internationally, contributing to policy and reform discussions on insolvency and restructuring.

The University of Texas at Austin
Strauss CENTER
for International Security and Law

23 AND YOU:
THE PRIVACY AND NATIONAL SECURITY IMPLICATIONS OF THE 23ANDME BANKRUPTCY

Prepared Statement of Adam I. Klein

Director, Robert Strauss Center on International Security and Law
University of Texas at Austin

Before the U.S. Senate Committee on the Judiciary

June 11, 2025

Chairman Grassley, Ranking Member Durbin, and Members of the Committee, thank you for inviting me to testify today. I last appeared here in 2022 to discuss the need to protect Americans' data from hostile foreign powers. This Committee's attention to the strategic value of Americans' data was prescient. Since then, Congress and the Executive Branch have taken several important steps to protect Americans' data. The Committee's attention to the 23andMe bankruptcy illustrates this heightened vigilance with respect to potential exports of sensitive personal data.

Below, I describe the national-security risks that would arise from bulk exports to China of American genomic data. These include possible use for intelligence operations and transnational repression, AI model training, biomedical research, and even bioweapons programs.

These risks illustrate an unfortunate reality of our geostrategic competition with the Chinese Communist Party. In an armed conflict over Taiwan, the CCP would likely seek to destabilize and immobilize American society with unconventional tactics aimed at the U.S. homeland. This hearing is a commendable example of what the 9/11 Commission called governmental "imagination": the ability to envision and preemptively address plausible threats, before they manifest. Congress must remain vigilant about other potential asymmetric tactics by the PRC and ensure that our intelligence agencies are equipped to detect and prevent them.

I. Bipartisan Progress on Exports of Sensitive Data to U.S. Adversaries

Under no circumstances should an entity controlled by or affiliated with the People's Republic of China (PRC) be permitted to buy 23andMe's genetic data. Allowing the data to fall into China's hands would pose several risks to U.S. national security, which I describe below in Part II. Fortunately, I am confident that the legal and regulatory structures erected in the past

several years, thanks to the work of this Committee and others in Congress, would prevent that from happening.[1]

Our government was not always so vigilant. Until recently, the Chinese Communist Party (CCP) exploited U.S. corporate bankruptcies to acquire sensitive American assets.[2] The CCP also used strategic investments and joint ventures to gain American technology and trade secrets.

Since then, Congress has dramatically improved our legal architecture for protecting sensitive American technology and data. New laws and regulations make it harder for the PRC to exploit American venture capital,[3] corporate bankruptcies,[4] and joint ventures with U.S. companies.[5]

Several laws and regulations now grant sensitive personal data similar protection. In the Foreign Investment Risk Review Modernization Act of 2018, Congress clarified the jurisdiction of the Committee on Foreign Investment in the United States to review foreign investments in American businesses that "maintain[] or collect[] sensitive personal data of United States citizens that may be exploited in a manner that threatens national security."[6]

Most recently, Congress addressed data-transfers outside of CFIUS's jurisdiction by enacting the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA), which bars data brokers from selling or otherwise transferring Americans' "sensitive personal data" to foreign countries and entities controlled by foreign adversary countries.[7] The law

---

[1] On April 17, 2025, the Department of Justice filed a "Notice Regarding Potential National Security Concerns" with the bankruptcy court. The notice strongly implies that a sale to a Chinese entity would be both subject to CFIUS review and prohibited by DOJ's Data Security Program, which I discuss below. Docket Entry 267 in No. 25-40976 (Bankr. E.D. Mo.). In addition, 23andMe has told Congress that it has "stipulated that no bids would be accepted from entities based in or with controlling investments from countries of concern, such as China…" Statement of Joseph Selsavage, Interim CEO and CFO, 23andMe, Holding Co., before the House Committee on Government Reform, Hearing on *Securing Americans' Genetic Information: Privacy and National Security Concerns Surrounding 23andMe's Bankruptcy Sale* 12 (June 10, 2025), https://oversight.house.gov/wp-content/uploads/2025/06/Selsavage-Written-Testimony.pdf.

[2] *See* Camille Stewart, *Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings*, 10 J. Nat'l Sec'y L. & Pol'y 277, 280-81 (2019) ("More to the point, China understands how to circumvent U.S. foreign investment regulations including by pressuring U.S. companies to enter joint ventures, by gaining access to assets through bankruptcy, and by coercing U.S. companies into sharing their capabilities and trade secrets.").

[3] *See* Executive Order 14105, *Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern* (Aug. 9, 2023); U.S. Dep't of the Treasury, Final Rule, *Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern*, 89 Fed. Reg. 90398 (Nov. 15, 2024); *see also* Presidential Memorandum, *America First Trade Policy*, Sec. (e) (Jan. 20, 2025) (ordering review of the EO and Final Rule to determine whether the order should be modified and whether the rule "includes sufficient controls to address national security threats").

[4] *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, § 1703, Pub. L. No. 115-232, 132 Stat. 1636, 2181 ("The Committee [on Foreign Investment in the United States] shall prescribe regulations to clarify that the term 'covered transaction' includes any transaction described in subparagraph (B) that arises pursuant to a bankruptcy proceeding or other form of default on debt.").

[5] *See*, e.g., Final Rule, *supra* note 3, at 90415 ("a *person of a country of concern* will be a *covered foreign person* by virtue of its participation in a joint venture with a U.S. person if such joint venture is engaged in a *covered activity*").

[6] Pub. L. No. 115-232, *supra* note 4, § 1703.

[7] Pub. L. No. 118-50, Div. I, 138 Stat. 960 (Apr. 24, 2024).

specifically defines "genetic information" as sensitive personal data subject to the prohibition.[8] PADFA is likely inapplicable here, however, as it generally excludes companies that collect data directly from their own customers.[9]

Finally, earlier this year, the Justice Department's Data Security Program, launched in April by the Trump Administration pursuant to an Executive Order by President Biden, broadened protection for sensitive bulk datasets and data that could be used to identify or compromise U.S. government employees.[10] The Data Security Program, unlike PADFA, applies not just to "third-party" data brokers, but also to "first-party" sellers who collected the information from their own customers. It also specifically prohibits transactions in human genomic data.[11]

Challenges remain, however. Foremost among them: the risk that, if purchases are foreclosed, adversary intelligence services will acquire the data by clandestine means. On their own, all but the most sophisticated private companies will struggle to fend off cyber penetrations from a first-tier adversary intelligence service. Tellingly, in 2023, hackers stole data on nearly 7 million 23andMe users.[12] Any service that aggregates sensitive personal data will offer an attractive target for adversary intelligence services. Improving our country's baseline level of cybersecurity, as the Strauss Center works to do through our Texas Cyber Clinic program,[13] can increase the cost and difficulty of such penetrations for foreign adversaries.

Human intelligence operations are another concern—especially with respect to China, which is known to maintain aggressive HUMINT operations in the United States. Compromised insiders with access to corporate systems can exfiltrate data, including sensitive bulk datasets, sought by PRC intelligence services.

Finally, effectively implementing PADFA and the Justice Department's Data Security Program will depend on companies to effectively vet their counterparties. The Data Security Program requires companies that engage in covered bulk-data transfers to maintain a compliance program, including due diligence before transactions and audits afterwards.[14] It remains to be

---

[8] *Id.* § 2(c)(7)(E).
[9] *See id.* § 2(c)(3)(A) ("The term 'data broker' means an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider.").
[10] *See* 28 C.F.R. Part 202; Executive Order 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (Feb. 28, 2024).
[11] *See id.* §§ 202.224 (defining "Human 'omic [sic] data"), 202.303 ("Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in any covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk U.S. sensitive personal data that involves bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived.").
[12] *See* 23andMe, Addressing Data Security Concerns – Action Plan (updated Dec. 5, 2023), https://blog.23andme.com/articles/addressing-data-security-concerns.
[13] *See* Robert Strauss Center for International Security and Law, University of Texas at Austin, *Texas Cyber Clinic*, https://www.strausscenter.org/apply-here-cyber-clinic/.
[14] *See* 28 C.F.R. §§ 202.1001, 1002.

seen whether these compliance programs will effectively prevent hostile foreign actors from purchasing sensitive datasets through front companies and other subterfuges.

The bottom line, however, remains quite positive. In just a few years, Congress and the Executive Branch, across multiple administrations, have dramatically improved legal protections around sensitive personal data, including genomic data. As this hearing illustrates, Congress and the Executive Branch are now on guard for major transfers that could create significant risks to our privacy and geostrategic interests.

II. The 23andMe Bankruptcy Illustrates a Major Shift in American Law and Policy: Sensitive Personal Data Must Not Flow to Geostrategic Adversaries

Cumulatively, these legal changes reflect a fundamental, welcome shift in the United States' approach to international data transfers. For decades, American policymakers aspired to preserve the ideal of an open internet where data moved freely across international boundaries. "Data localization" requirements were seen as inconsistent with that vision of the internet as inherently global and borderless.

That view was not universally shared. The European Union, for instance, has long barred data transfers unless the receiving country offers an "adequate level of protection," as determined by the European Commission in the first instance and ultimately by the Court of Justice of the European Union.[15] Ironically, that "adequacy" principle has been most aggressively applied to data-transfers to the United States, a treaty ally of most EU member states. In a welcome recent turn, however, the Irish Data Protection Commissioner has turned its attention to transfers to China, whose approach to personal privacy is fundamentally incompatible with that of rule-of-law systems.[16]

In recent years, however, U.S. policy has shifted decisively: America's leaders, of both parties and both policymaking branches, now embrace the principle that sensitive American data should not flow to U.S. adversaries.

That is the only sound choice in an era of intense geostrategic competition. As I have previously argued, the Chinese Communist Party "holds a fundamentally different vision of politics, global order, and human flourishing. Data flows from the United States can help the CCP achieve that vision and subvert ours."[17]

Data is not a commodity like any other: sensitive data can have powerful strategic implications. Personal data can help adversaries customize and target clandestine intelligence operations and propaganda campaigns. Large datasets can also help adversaries like China train AI models and develop products to displace U.S. competitors and strengthen their militaries.

---

[15] *See* EU Directive 95/46, art. 25; Gen'l Data Protection Reg., arts. 44-45.
[16] *See* Data Protection Comm'n of Ireland, *Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China* (May 2, 2025), https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following.
[17] *See* Testimony of Adam Klein before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, *Protecting Americans' Private Information from Hostile Foreign Powers* (Sept. 14, 2022).

III. Bulk Transfers of U.S. Genomic Data Would Create Unacceptable Risks to National Security

Thankfully, heightened vigilance and the legal reforms described above make it unlikely that federal authorities would permit a PRC-affiliated entity to purchase 23andMe or its records.[18] Nonetheless, it bears revisiting the risks that bulk transfers of genomic data to China would pose to our national security.

Intelligence Operations and Transnational Repression

PRC intelligence services have already stolen massive quantities of sensitive data from the U.S. Office of Personnel Management and private companies like Marriott, Equifax, and Anthem.[19] Large datasets like these can be combined and analyzed to identify our intelligence officers, target those in possession of defense or industrial secrets for recruitment, and gain access to other sources of information.

Genomic data presents distinctive risks. Intelligence services can use DNA profiles to identify people of interest. While publicly available information is limited, the U.S. government reportedly collected DNA samples from counterterrorism detainees, enabling agencies to reliably identify terrorism suspects in future encounters.[20] And it is well known that the FBI and other agencies collect DNA from arrestees and convicts for law-enforcement purposes.

PRC intelligence services might seek to exploit genomic information in various ways.[21] DNA profiles could be used to reliably identify (or, if a profile indicated a health vulnerability) to target or coerce Americans of interest. DNA profiles might also help PRC officials identify and target overseas Chinese for recruitment or transnational repression, perhaps by identifying family connections based on genomic profiles.

Biomedical Research and AI Models

For years, Chinese companies and government agencies have "collect[ed] genetic data from around the world, part of an effort by the Chinese government and companies to develop the world's largest bio-database."[22] That could give Chinese companies an advantage in AI-

---

[18] *See supra* note 1.
[19] Department of Justice, *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax* (Feb. 10, 2020) ("For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax.").
[20] *See* Homeland Security News Wire, *Pentagon maintains a DNA database with 80,000 DNA profiles*, Dec. 15, 2008, https://www.homelandsecuritynewswire.com/pentagon-maintains-dna-database-80000-dna-profiles.
[21] *See* National Counterintelligence and Security Center, *Protecting Critical and Emerging U.S. Technologies from Foreign Threats* 6 (Oct. 2021) ("Large genetic databases that allow people's ancestry to be revealed and crimes to be solved also can be misused for surveillance and societal repression.").
[22] Julian Barnes, *U.S. Warns of Efforts by China to Collect Genetic Data*, N.Y. Times, Oct. 22, 2021.

powered biomedical research, which promises great economic rewards and elevated global influence to the countries that lead in it.[23]

Both the United States and China are racing to gain the edge in developing "frontier" AI models. Training these models requires vast amounts of high-quality training data. The more data, the better the result. China, of course, generates immense quantities of data, and its national DNA database reportedly holds nearly 70 million profiles. But profiles generated within China pertain primarily to Chinese citizens of "Han" Chinese ancestry.

Models trained on China's own genomic data thus may not be predictive when applied to the U.S. population, which is much more ethnically diverse. There is precedent for this: the National Institute of Standards and Technology found that facial recognition models developed in China had lower false-positive rates on East Asian faces,[24] an effect almost certainly attributable to the composition of the training data. Gaining access to a large volume of U.S. genomic data would help China train specialized models that would be more predictive across genetically diverse populations.

Bioweapons

China could also use U.S. genomic data to pursue biomedical research with offensive or malign intent. This prospect is speculative, and may seem farfetched, but we should not dismiss it. China's history with dangerous "gain of function" research at the Wuhan Institute of Virology is well-documented.[25] And the House Select Committee on the CCP recently described how, in 2022, officials uncovered an illegal, secret biolab in California, with "thousands of vials" containing serious biohazards and a refrigerator labeled "Ebola."[26] The lab was run by a PRC citizen with ties to China's civil-military fusion program.[27]

Warning signs continue to emerge. Last week, the Department of Justice indicted two PRC citizens for trying to smuggle the crop fungus *Fusarium graminearum*, classified as a potential agroterrorism weapon, into the United States.[28] A third PRC citizen was indicted separately this week for attempting to smuggle a "biological material related to roundworms" across our borders.[29]

---

[23] *See* National Counterintelligence and Security Center, *supra* note 21, at 6 ("large bodies of data – such as patient health records or genetic sequence data – represent long-term, unrealized development of products and applications").
[24] Patrick Grother et al., National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects* 2 (Dec. 2019).
[25] *See, e.g.*, U.S. Department of State, Fact Sheet: Activity at the Wuhan Institute of Virology (Jan. 15, 2021), https://2017-2021.state.gov/fact-sheet-activity-at-the-wuhan-institute-of-virology/.
[26] U.S. House of Representatives, Select Committee on the Chinese Communist Party, *Investigation into the Reedley Biolab* 3 (Nov. 2023).
[27] *Id.* at 17-20.
[28] U.S. Attorney's Office for the Eastern District of Michigan, *Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the U.S. for their Work at a University of Michigan Laboratory* (June 3, 2025), https://www.justice.gov/usao-edmi/pr/chinese-nationals-charged-conspiracy-and-smuggling-dangerous-biological-pathogen-us.
[29] U.S. Attorney's Office for the Eastern District of Michigan, *Alien from Wuhan, China, Charged with Making False Statements and Smuggling Biological Materials into the U.S. for Her Work at a University of Michigan*

Large volumes of U.S. genomic data could help China predict how bioweapons would affect the U.S. population, including particular ethnic groups.[30] The PRC is known to have developed a genetic database to monitor its own Uyghur minority population, in part by forcing Uyghurs to give DNA samples at mandatory "medical checkups."[31] And authoritarian regimes with similarly racialized policies have sought ethnically targeted bioweapons in the past: South Africa allegedly sought to develop "an anti-fertility vaccine that would selectively target the Black majority."[32]

Disturbingly, the Chinese military appears open to the possibility of ethnically targeted weapons. According to Craig Singleton of the Foundation for Defense of Democracies, an official People's Liberation Army textbook on the "Science of Military Strategy … noted how new kinds of biological warfare, including 'specific ethnic genetic attacks,' could be used against entire racial and ethnic groups."[33] AI models trained on U.S. genomic datasets could accelerate PRC efforts to develop such a weapon.

IV. We Must Anticipate and Detect Other Asymmetric Tactics by the PRC

In the PRC, the United States faces perhaps the most formidable peer competitor in our history. China's economic, industrial, and scientific prowess far outstrip what the moribund Soviet economy could achieve in any of those domains. Meanwhile, the PRC exploits our open society to conduct industrial espionage, transnational repression, and clandestine influence. The risk of armed conflict, likely around Taiwan, will only intensify as Xi Jinping's 2027 deadline for the People's Liberation Army to be ready to take Taiwan approaches.

In an armed conflict over Taiwan, we should not expect China to fight us only in the places and ways for which we have prepared. Instead, we must anticipate and prepare for the unexpected. The 9/11 Commission called this "imagination"; its landmark report painstakingly documented how the U.S. government failed to treat al Qaeda as a potentially catastrophic threat or to envision mass-casualty suicide hijackings.[34] Congress's concern about sales of U.S. genomic data to China is an example of such imagination.

In a conflict with China, we should expect other unconventional tactics that strike at the vulnerabilities of our open society. Such tactics could include:

Laboratory (June 9, 2025), https://www.justice.gov/usao-edmi/pr/alien-wuhan-china-charged-making-false-statements-and-smuggling-biological-materials.

[30] *See* National Counterintelligence and Security Center, *supra* note 21, at 6 ("Genomic technology used to design disease therapies tailored to an individual also can be used to identify genetic vulnerabilities in a population.").

[31] *See* Sui-Lee Wee, *China Uses DNA to Track Its People, With the Help of American Expertise*, N.Y. Times, Feb. 21, 2019 (Collecting genetic material is a key part of China's campaign, according to human rights groups and Uighur activists. They say a comprehensive DNA database could be used to chase down any Uighurs who resist conforming to the campaign."); *see also* Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. Times, Apr. 14, 2019 (describing development of facial-recognition algorithms capable of identifying Uyghurs).

[32] Jerome Amir Singh, *Project Coast: Eugenics in Apartheid South Africa*, 32 Endeavour 5, 6 (2008).

[33] Craig Singleton, *Biotech Battlefield Weaponizing Innovation in the Age of Genomics*, Foundation for Defense of Democracies, at 11-12 (January 2021), https://www.fdd.org/wp-content/uploads/2025/01/fdd-monograph-biotech-battlefield-weaponizing-innovation-in-the-age-of-genomics.pdf.

[34] *See* National Commission on Terrorist Attacks Upon the United States, *Final Report*, ch. 11 (2004).

- Mass drone attacks launched from within the U.S. homeland or just offshore.
- Targeted TikTok campaigns to demoralize Americans, incite social unrest, or suborn members of the military or critical industries.
- Cyber or biological attacks on our food or water systems.
- Market manipulation or cyberattacks designed to cause financial panic.

Preventing catastrophic surprises like these, or others yet unimagined, will require exquisite intelligence on PRC plans, intentions, and emerging capabilities. In that vein, it bears noting that this Committee will be called upon next year to consider once again whether to reauthorize Section 702 of the Foreign Intelligence Surveillance Act (FISA). In recent years, the government's use of FISA has attracted searching oversight and proposals for reform,[35] many of which were adopted by Congress in the last reauthorization. Next year's reauthorization will provide an opportunity to consider further changes—including, perhaps, more fundamental reforms to make FISA a more effective, targeted national-security tool while reducing the risk to Americans' civil liberties.

Allowing Section 702 to sunset, however, would make it easier for China to plot and execute an asymmetric surprise attack on our homeland without being detected. For example, if China were covertly exfiltrating American genomic data and using it for bioweapons research or AI training, we would rely on our intelligence agencies to warn policymakers and develop countermeasures.

Thank you for the opportunity to testify today. I look forward to your questions.

[35] *See, e.g.*, Adam I. Klein, Chairman, U.S. Privacy and Civil Liberties Oversight Board, *Chairman's White Paper: Oversight of the Foreign Intelligence Surveillance Act* (June 2021), https://documents.pclob.gov/prod/Documents/EventsAndPress/ec2bfc95-f111-4123-87d5-8a7827bf2fdd/Chairman's%20FISA%20White%20Paper.pdf.

#
23andMe Holding Co.#
;:3#P dunhw#Vwhhw#Urrp #748#
Vdq#udqf\rfr/#PD#k73;9#
#
1qirC 56dqgp h1frp #
z z z 356dqgp h1frp #

Statement of Joseph Selsavage
Interim Chief Executive Officer and Chief Financial Officer, 23andMe Holding Co.
Hearing: 23 and You: The Privacy and National Security Implications of the 23andMe Bankruptcy
Senate Committee on the Judiciary

June 11, 2025

Chairman Grassley, Ranking Member Durbin, other members of the Committee, thank you for the opportunity to appear before you today. My name is Joseph Selsavage, and I represent 23andMe, a mission-driven organization founded on a simple yet transformative belief: that individuals have the right to access, understand, and benefit from their own genetic information. I came to 23andMe in November 2021, when the company acquired Lemonaid Health, where I had been Chief Financial Officer since joining in 2020. As of March 23, 2025, I have been serving as the Interim Chief Executive Officer of 23andMe.

From the very beginning, 23andMe's purpose has been clear: to help people live healthier lives through direct access to their own DNA, to accelerate scientific discovery, and to contribute meaningfully to the future of personalized medicine. We recognize that with this vision comes immense responsibility—to our customers, to public health, and to the trust we are granted by millions of individuals who have chosen to participate in something larger than themselves.

We are here today not only to answer your questions, but to reaffirm our deep commitment to data privacy and security, transparency, customer choice, data stewardship, and scientific integrity. At a time when science and technology are evolving faster than policy and public understanding, it is essential that companies like ours lead with accountability.

As we share our perspective with the Committee today, we do so with humility, with a clear view of the challenges ahead, and with an unwavering focus on our mission: to empower every person with access, understanding and the ability to benefit from their DNA, while safeguarding the principles of ethics, privacy, and security that must guide innovation in the 21st century.

Background on 23andMe

Founded in 2006, 23andMe is a personal genomics and biotechnology company that pioneered direct-to-consumer genetic testing. We are named after the 23 pairs of chromosomes in every human cell. 23andMe is a saliva-based DNA service that provides customers with information about their ancestry and important health information.

Our mission has always been to empower consumers by providing access to information about their personal genetics based on the latest science, so they can make their own informed decisions about their healthcare journey. We believe the information provided by direct-to-consumer genetic tests provides a starting point for individuals to consider various choices, including lifestyle changes that could help them reduce potential genetic health risks about which they may never have been aware through the traditional healthcare system. We have worked for 19 years to translate complex genetic science into actionable, understandable insights, empowering individuals to make informed decisions.

As one of the first and only companies to receive FDA authorization for direct-to-consumer genetic health reports, we helped democratize access to personal genomic information. Our mission is for all people to

be able to *access*, *understand* and *benefit* from their DNA. We have over 13 million customers globally, many of whom have used our service to connect with family members, discover their roots, and gain insights into health risks, traits, and inherited conditions. Our services allow customers to gain DNA insights about their genetic risk for dozens of conditions like Type 2 diabetes, Alzheimer's disease, and certain cancers. They can also learn about their carrier status for inherited conditions like cystic fibrosis or Tay-Sachs disease, or wellness factors like lactose intolerance or deep-sleep tendencies. 23andMe customers have consistently reported taking positive health action after learning about their genetics through 23andMe's services. Based on surveys, 82% of customers with an actionable genetic result were previously unaware of their health risks, and after receiving their report, 86% of customers who shared results with their doctors received at least one medical recommendation, and 87.5% of those recommendations were followed.[1]

Additionally, more than 4 million customers have found they have a higher likelihood of Type 2 diabetes; more than 2.2 million customers have learned they have a higher likelihood of coronary artery disease; more than 1 million customers have found they are at high genetic risk for harmful blood clots (hereditary thrombophilia); and more than 28,000 customers have been identified as having BRCA1/BRCA2 variants which indicates up to an 85% lifetime risk for breast cancer and increased risk for ovarian and other cancers.

The Registration Process

The process for our services was built to be easy for everyone over the age of 18 to complete: You order a kit from 23andMe.com or a retailer like Amazon or Walmart.com. Once you receive a kit, you create an account online and register your kit's barcode on 23andMe's website or its mobile app. After registering,

[1] Based on 2023 survey, designed by 23andMe Genomic Health & Sciences, of 1,076 23andMe research-consented participants with variants in *BRCA1, BRCA2, APOB, LDLR, HFE, TTR, MUTYH*.

you submit a saliva sample using a small tube provided in the kit. The sample is sent to a CLIA-certified laboratory using prepaid packaging. The registration process is designed to ensure a new customer's sample is connected to their account in a way that protects their privacy. The barcode number customers use to register their kit ensures the processing lab does not receive any personally identifying information and that the data is linked to the correct individual.

After a sample arrives at the lab, it takes roughly 4 to 6 weeks to process, and customers can find up-to-date information by logging into their 23andMe account. Once the DNA is processed, customers receive reports through our secure online platform.

There are four types of services we offer today:

1. Ancestry Service: Our Ancestry Service is the most comprehensive ancestry breakdown available with 80+ personalized reports, ancestry composition across 4000+ geographic regions, ancestry percentages (to the 0.1%), 30+ trait reports and has the ability to upgrade to the health services at any time.

   Our Ancestry Service helps customers understand who they are, where their DNA comes from and their family story. It breaks down their ethnic background, shows their genetic ancestry by region, and traces their maternal and paternal lineage. If they choose to participate in the DNA Relatives features, customers can connect with other customers with whom they share DNA—their genetic relatives.

2. Health & Ancestry Service: Our Health & Ancestry service includes everything in the Ancestry Service, plus 150+ personalized reports which include FDA-authorized reports. This service is

FSA/HSA eligible. Report examples include: increased risk for conditions like Type 2 diabetes, late-onset Alzheimer's disease, and BRCA1- and BRCA2-related cancers.

3. 23andMe+ Premium Service: An annual subscription service includes everything in our Health & Ancestry Service. This service includes advanced, premium features, reports and tools for ancestry and health related data. This service is FSA/HSA eligible.

   23andMe+ Premium offers everything from our Health + Ancestry kit as well as more than 40 additional health predisposition reports on common conditions (e.g. heart health) based on polygenic risk scores (PRS), pharmacogenetics reports that help customers learn how they may process certain medications. Premium offers ongoing access to new reports as they are developed.

4. 23andMe+ Total Health: Our most advanced service providing next generation sequencing genetic reports and includes blood testing and access to genetics-based clinical care. This service is FSA/HSA eligible. This service covers 200x more hereditary disease-causing variants than our personal genome service reports (50,000+ variants in Total Health exome sequencing compared to 250 in Carrier Status and Genetic Health Risk reports). It is an annual subscription. Total Health gets its name from adding essential bloodwork and genetics trained clinician discussions to the service, to get an advanced, integrated understanding of your health risks.

Providing health data to our customers is something we take very seriously at 23andMe. We implemented educational and comprehension-based tutorials before providing access to specific reports. Customers must specifically opt in to receiving reports for Parkinson's and Alzheimer's. These explicit opt-ins are in addition to the initial company consents, meaning customers cannot access or view these reports until they take this action. We also have educational tutorials for BRCA, HOXB13 (hereditary prostate cancer),

and MUTYH (hereditary colorectal cancer) cancer reports, as well as for general carrier status, genetic health risks, and pharmacogenetic report categories that customers *must view before* accessing those categories of reports.

Customer Stories

We have many powerful customer stories that highlight the profound impact genetic insights can have on people's lives—often uncovering health risks, prompting critical medical action, and enabling proactive decisions that change the course of individuals' futures Below are a few examples that customers have shared with us.

At 31, Casey didn't expect his health reports to reveal anything significant—but they did. He discovered he carried two copies of a variant linked to hereditary hemochromatosis, a condition that can lead to dangerous iron overload. Follow-up bloodwork and imaging confirmed elevated iron levels and mild liver toxicity. Thanks to early detection, Casey is now under specialist care and undergoing regular phlebotomy to manage the condition.

Ashley, a 33-year-old mother, discovered she had a BRCA1 variant through her genetic health report. Despite her young age and no known family history, Ashley insisted on further screenings—requests that were initially dismissed. Her persistence paid off: she was diagnosed with stage two triple negative breast cancer, a fast-moving form closely tied to BRCA1. Her doctors told her that without early detection, it might have been found much later, when treatment options would be more limited.

Similarly, Gina was unaware of her Ashkenazi Jewish ancestry or any breast cancer history. But her 23andMe report revealed a BRCA1 variant, prompting her to consult with medical experts and eventually undergo a prophylactic double mastectomy and hysterectomy. Navigating this during the height of the

COVID-19 pandemic, Gina faced her journey with courage—and now uses her experience to advocate for others through her blog and speaking engagements.

Dana's story further illustrates how genetic knowledge can uncover critical connections. Though she had a family history of pancreatic cancer, she didn't know it was linked to the BRCA gene—or that her Ashkenazi Jewish heritage meant a 1 in 40 chance of carrying the mutation. Just four months after reviewing her reports, she confirmed her BRCA status through additional testing and underwent preventive surgeries that dramatically reduced her risks for both breast and ovarian cancer.

As a 57-year-old adoptee, Laura lacked access to her biological health history. Genetic testing revealed a heightened risk for nonalcoholic fatty liver disease (NAFLD), particularly among women with her genetic profile. After experiencing chronic symptoms, she worked with her physician to confirm the condition and is now taking active steps—including working with a nutritionist and exercising regularly—to manage it before it progresses.

Rebecca learned she carries one copy of the APOE ε4 gene, associated with an increased risk for late-onset Alzheimer's disease. Motivated by this information, she enrolled in clinical trials and began treatment with Leqembi®, just before its FDA approval. Her sister, who shares the same genetic variant, now joins her for biweekly infusion therapy—an example of how these insights can benefit entire families.

Andrew's experience shows how genetic insights can become urgently relevant. After learning he carried a variant in the F2 gene associated with blood clots, his father suddenly collapsed due to massive clots in his heart and lungs. Andrew shared his results with doctors, who confirmed his father also carries the variant. This diagnosis has since helped guide preventative care for both of them.

These are only some of the many, hundreds of stories that illustrate the power of genetic testing. These individuals have not only taken control of their own health but have also paved the way for others to do the same (https://www.23andme.com/stories/).

Powering Research and Scientific Publications

The value of personal genomics goes beyond the insights people learn about themselves. Customers who submit their DNA for analysis also have the option to allow their data to be shared for research purposes—and over 80% choose to consent to research. Since 2010, 23andMe has published 293 papers (https://www.23andme.com/publications/).

Consent is a central tenet of 23andMe's Research program. We have separate research consents, beyond our processing sensitive data consent, Privacy Statement, and terms of service, that customers must review and agree to if they want to participate in our Research program. These consent documents are subject to the review and oversight of our external and independent Institutional Review Board (IRB), which ensures that the risks and benefits of participation in research are properly presented to the potential participant so they can make an informed decision about participation.

Customers who affirmatively consent contribute to more than 230 studies on topics that range from Parkinson's disease to lupus to asthma and more. We collaborate with biotech companies, advocacy organizations and universities to bring customers opportunities to participate in research. Participants can spend anywhere from five to 50 minutes—the choice is theirs—answering online survey questions that enable researchers to combine their genetic information with millions of other data points to help drive scientific and medical discoveries.

23andMe has received grants from the U.S. National Institutes of Health to fund research and data voluntarily provided by 23andMe's customers has led to the identification of hundreds of new genetic

associations, including associations with Parkinson's disease, depression, and skin cancer. We collaborate with some of the best and brightest talent in the world of genetics research—including researchers at the University of Chicago, Stanford University and the Broad Institute, as well as the Lupus Research Institute, the Michael J. Fox Foundation and Sickle Cell 101, among others—and our findings are regularly published in leading peer-reviewed scientific journals, such as *Science*, *Nature*, and the *New England Journal of Medicine*. In addition to working with partners that focus on drug development, 23andMe previously conducted its own research to try to identify new therapies for both common and rare diseases.

Our commitment is to responsibly harness the power of DNA to benefit human health and advance scientific understanding.

How We Ensure Customer Data is Protected and Their Preferences Honored

Our customers can make their own choices about how their data is used and whether 23andMe retains their information. Customers' data is not shared for research purposes unless the customer affirmatively consents—and we remove all identifying information before genetic data is shared unless specifically consented for limited purposes. Any customer who affirmatively consents to participate in our Research program can easily opt out at ANY time through their account settings—and always has been able to do so. Customers are also free to delete their accounts and all the information we retain at any time.

From the beginning, privacy and empowerment have been central to 23andMe's business. Our systems ensure that genetic data is stored separately from personal identifiers; and users control their information—including having the ability to decide whether to participate in research, share information with DNA matches, or download their raw data.

We have a strong security program that includes encryption, access controls and regular audits. We comply with applicable regulatory requirements.

We follow strict security protocols and privacy principles, including:

- **Explicit Consent:** We never share individual-level data without the user's consent.
- **Transparency:** We clearly communicate how data is used and give customers control over their data sharing preferences.
- **Data Storage:** All research data is stored separately from any identifying information to protect customer privacy.
- **Security Standards:** We use industry-standard encryption, access controls, and monitoring systems to protect data.

However—despite our best efforts—we know that no system is infallible.

In October 2023, we learned that a threat actor accessed individual 23andMe.com accounts through a process called *credential stuffing*. This is the automated injection of stolen username and password pairs ("credentials") into website login forms to fraudulently gain access to user accounts. The threat actor was able to access approximately 14,000 user accounts in instances where usernames and passwords that customers used on the 23andMe website were the same as those used on other websites that had been previously compromised and then made available online. Using this access to the credential stuffed accounts, the threat actor was able to access limited customer profile information for over 6 million users, which the customers had chosen to share with other genetic relatives when they decided to participate in 23andMe's DNA Relatives feature.

Upon discovery of the security incident, we took immediate action. We disabled impacted accounts and temporarily disabled the "DNA Relatives" feature. We forced password resets for all users. We engaged leading cybersecurity firms to conduct a full forensic investigation. We notified law enforcement,

regulators and affected customers, in compliance with applicable laws. And we enhanced login security by implementing mandatory two-factor verification for all accounts.

We acknowledge the seriousness of the security incident and the anxiety it caused our customers, which we deeply regret. We are committed to continued transparency, security, and maintaining trust among customers.

Process Going Forward

23andMe's bankruptcy was driven by a variety of factors including the aforementioned security incident, macroeconomic headwinds affecting biotech companies, and a strategic reassessment of our operational model. Due to these circumstances, the company made the difficult decision to voluntarily file for Chapter 11 bankruptcy protection in March of this year to facilitate a sale, with the aim of maximizing the value of the business for its stakeholders.

During this process we continued to operate as usual. There has been no disruption to any service or offering we provide. Customers have been able to continue to purchase kits, access to data remained has unchanged, and we have continued offering and fulfilling subscriptions. We have made no changes to how we store, manage or protect customer data. We've made no changes to our privacy policies or to how customers can manage their preferences. Customers have been able to delete their data at any time, and no changes to our data deletion policy were made.

Throughout the sale process, we have sought to secure a partner that shares our commitment to customer data privacy and that will continue our mission to help people access, understand and benefit from knowledge about the human genome. We are requiring that any buyer agree to comply with existing 23andMe privacy policies and applicable law with respect to the treatment of customer data.

We also have stipulated that no bids would be accepted from entities based in or with controlling investments from countries of concern, such as China, Cuba, Iran, North Korea, Russia or Venezuela, which would have raised concerns around customer privacy and national security.

In addition, we asked the court to appoint an independent Customer Data Representative (CDR) to serve as an independent third party, reviewing whether any proposed transaction complied with our privacy policies and applicable data privacy laws and maintained customer data security. We made this request proactively and before any other party, including our regulators, made a similar request.

23andMe, the Official Committee of Unsecured Creditors (UCC), the U.S. Trustee, and 32 state attorneys general ultimately agreed to the appointment of a disinterested Consumer Privacy Ombudsman (CPO) with privacy and cybersecurity credentials to conduct an examination and present a report to the bankruptcy court, evaluating a potential bidder's privacy and security program and assessing the impact of any potential sale on the protection of consumer data.

As Congress is aware, we have run a successful sale process and are presently down to two bidders—biotech company Regeneron and the nonprofit medical research organization TTAM Research Institute. Both are American enterprises. Pursuant to a bankruptcy court order, and with the agreement of the parties, there will be a subsequent round of bidding prior to the sale hearing, which is currently set for June 17, 2025. Because this process is ongoing, I am unable to speak to the merits of either bid or the ongoing sale process.

But two points bear repeating:

- First and foremost, privacy and data security remain one of our top priorities. We remain committed to protecting sensitive customer data. We require anyone bidding for 23andMe to agree to comply with our privacy policies and all applicable privacy laws.

- Second, there have been no changes to customer access to accounts, genetic reports, or any stored data and no change to customers' ability to control their accounts, including the ability to delete their data.

In closing, we recognize the vital importance of protecting every individual's right to access and control their own genetic information. Empowering people with knowledge about their DNA is not only a matter of personal autonomy—it is a gateway to proactive and personalized health, informed decision-making, and greater engagement in scientific progress. At 23andMe, we believe that when consumers are trusted with their own data, they become partners in advancing healthcare, not just patients of it.

I appreciate the opportunity to testify before the Committee today and welcome your questions.

A P P E N D I X

The following submissions are available at:

https://www.govinfo.gov/content/pkg/CHRG-119shrg61889/pdf/CHRG-119shrg61889-add1.pdf

Submitted by Chairman Grassley:

Submitted by Ranking Member Durbin:

○