SECURING AMERICANS' GENETIC INFORMATION: PRIVACY AND NATIONAL SECURITY CONCERNS SURROUNDING 23ANDME'S BANKRUPTCY SALE

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JUNE 10, 2025

Serial No. 119–32

Printed for the use of the Committee on Oversight and Government Reform

Available on: *govinfo.gov, oversight.house.gov* or *docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

60–682 PDF WASHINGTON : 2025

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
ELI CRANE, Arizona
BRIAN JACK, Georgia
JOHN MCGUIRE, Virginia
BRANDON GILL, Texas

VACANT, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
EMILY RANDALL, Washington
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona
WESLEY BELL, Missouri
LATEEFAH SIMON, California
DAVE MIN, California
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

MARK MARIN, Staff Director
JAMES RUST, Chief Counsel for Oversight
MITCH BENZINE, General Counsel
MARGARET HARKER, Senior Advisor
ELLISON TOLAN, Counsel
SHARON UTZ, Senior Professional Staff Member
CHARLES DONAHUE, Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JAMIE SMITH, Minority Staff Director
CONTACT NUMBER: 202-225-5051

C O N T E N T S

OPENING STATEMENTS

WITNESSES

Written opening statements and bios are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

The documents listed are available at: docs.house.gov.

ADDITIONAL DOCUMENTS

These documents were submitted after the hearing, and may be available upon request.

SECURING AMERICANS' GENETIC INFORMATION: PRIVACY AND NATIONAL SECURITY CONCERNS SURROUNDING 23ANDME'S BANKRUPTCY SALE

TUESDAY, JUNE 10, 2025

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
Washington, D.C.

The Committee met, pursuant to notice, at 10:02 a.m., in HVC–210, U.S. Capitol Building, Hon. James Comer [Chairman of the Committee] presiding.

Present: Representatives Comer, Gosar, Foxx, Grothman, Cloud, Palmer, Higgins, Sessions, Biggs, Perry, Timmons, Burchett, Greene, Luna, Burlison, Crane, McGuire, Gill, Norton, Lynch, Krishnamoorthi, Mfume, Brown, Stansbury, Frost, Lee, Crockett, Randall, Subramanyam, Bell, Min, Pressley, and Tlaib.

Chairman COMER. Filling in throughout the Committee hearing because people stayed up all night watching America's team, Murray State, beat Duke to go to the College World Series, so people will be in momentarily.

I recognize myself for the purpose of making an opening statement.

OPENING STATEMENT OF THE CHAIRMAN JAMES COMER, REPRESENTATIVE FROM KENTUCKY

I want to welcome everyone to today's Committee hearing on the privacy and national security concerns surrounding 23andMe bankruptcy sale. 23andMe is a direct-to-consumer genetic testing company in possession of personal genetic data of millions of Americans. On March 23, 2025, the company voluntarily filed for Chapter 11 bankruptcy, leaving open the question of who will purchase 23andMe and who may gain access to the sensitive information of customers and their family members.

On May 19, 2025, Regeneron Pharmaceuticals, a biotechnology company based in New York, announced that it had entered into an asset purchase agreement to acquire 23andMe. On June 4, 2025, the court decided to reopen the auction for 23andMe to allow for final bids from Regeneron, TTAM Research, and let me note that TTAM was founded by 23andMe co-founder and former CEO, Ms. Anne Wojcicki. With over 15 million customers worldwide, 23andMe uses a saliva sample to uncover their ancestry, family traits, and potential health risks. To whoever ends up controlling

the company, there are serious concerns about what will happen to this private information. How will it be stored? What will it be used for? Could it end up in the hands of a foreign adversary through direct investment or indirectly through future partnerships? Could the information be used against customers and consumers?

23andMe has a record of engaging with foreign adversaries, namely the Chinese Communist Party (CCP). In 2015, the company received $115 million in funding from investors, including WuXi Healthcare Ventures, which was then a corporate venture arm of WuXi AppTec, a company with ties to the CCP and Chinese People's Liberation Army. At the time, the investment valued 23andMe at $1.1 billion. According to 23andMe, this partnership was terminated, but questions remain about the potential for the future owner of the company to partner with bad foreign actors. Notably, Regeneron partnered with a Chinese company called Zai Lab Limited on drug clinical trials during the height of the COVID pandemic.

It is well known that the CCP engages in mass surveillance and has conducted dangerous activities to advance bio weapons, both used against its critics. In fact, 23andMe was hacked in 2023, exposing personal information from nearly seven million profiles, mostly targeting Jewish and Chinese customers. The *New York Times* reported that China and other countries are working to dominate these technologies and are using both legal and illegal means to obtain American expertise. The CCP has a history of misusing genetic data, including DNA tests to track Uyghur Muslims.

National security concerns about 23andMe are not new. In December 2019, the U.S. Department of Defense advised members of the military not to use consumer DNA kits, saying the information collected by private companies could pose a security risk. A DOD memo warned that consumers' DNA kits pose personal and operational risks to service members and raised concerns about outside parties using genetic data for mass surveillance and unauthorized tracking. It is imperative that 23andMe and other companies like it ensure there is absolutely no legal or illegal way for foreign adversaries or anyone else to access, manipulate, and abuse Americans' genetic data to advance their nefarious agendas.

Potential harm for consumers does not come solely from hostile foreign actors. Disclosures of individuals' genetic data could also be used for assessing higher insurance premium, restrictions on credit extensions by financial institutions, and targeted advertising based on predisposition to specific medical conditions. All of this raises concerns about whether Congress needs to take action to ensure safety of Americans' personal genetic data. Given these serious risks, I look forward to hearing from the co-founder, former CEO, and current board member of 23andMe, who is bidding in the bankruptcy sale, Ms. Anne Wojcicki and interim CEO, Mr. Joseph Selsavage.

As previously discussed with the witnesses, the Committee is aware of some court-mandated restrictions on public disclosure of specific aspects of the ongoing bankruptcy proceedings. It is our understanding that these restrictions are limited and not applicable to all aspects of the pending bankruptcy. The Committee expects

the witnesses to answer the questions to the fullest extent possible. And with that, I yield to Ranking Member Lynch for his opening statement.

Mr. LYNCH. Thank you, Mr. Chairman, and I want to thank the witnesses for their willingness to come before the Committee and help us with our work.

OPENING STATEMENT OF RANKING MEMBER STEPHEN LYNCH, REPRESENTATIVE FROM MASSACHUSETTS

Mr. LYNCH. Chairman Comer, thank you for calling this hearing to examine the very serious issue of how we can protect Americans' sensitive personal data from hostile actors. 23andMe holds the genetic and biographical data of 15 million customers. This includes billions of phenotypic data points that make up DNA profiles, detailed genealogical and ancestry history, and importantly, health predispositions. While healthcare providers and insurance companies must follow Federal laws like the Health Insurance Portability and Accountability Act, or HIPAA, which protects patients' sensitive data from unauthorized sharing, direct-to-consumer companies like 23andMe operate with minimal oversight and regulation. The lengthy and opaque terms of service and privacy policies that customers are required to agree to typically allow for their data to be sold during a sale or bankruptcy, and that is precisely the situation that millions of the company's customers find themselves in today.

Americans deserve to know what the sale of 23andMe will mean for sensitive genetic data it holds. Unfortunately, Chairman Comer has demanded this hearing take place today, unfortunately, in the midst of the bankruptcy bidding process when these witnesses are legally prohibited in some respects from speaking to any details related to the bankruptcy and sale, but we will do our best together to get answers despite this challenge. Our concerns are magnified by the fact that the hostile actors, including foreign adversaries, are constantly attempting to buy or steal Americans' sensitive data.

In 2023, 23andMe was the target of a massive breach in which an outside attacker stole the data of seven million customers, reportedly targeting those with Ashkenazi Jewish heritage. The governments of the People's Republic of China, the Russian Federation, North Korea, and Iran conduct persistent cyberattacks against the United States. China's president, Xi Jinping, has made clear that dominating the AI race and achieving global supremacy in biotechnology are critical to the future geopolitical power, and obtaining vast troves of Americans' sensitive data is a key component of this strategy. Failing to safeguard Americans' data from these hostile actors would not only be a critical violation of privacy, but also a national security catastrophe. Given the sensitive nature of the data that companies like 23andMe hold, the possibility for that data to end up in entirely new hands in the event of a sale or bankruptcy and the risk of data breaches, including by hostile foreign governments, we cannot rely solely on corporate efforts to ensure this data is protected. We need strong privacy protections and comprehensive laws and regulations that address the evolving landscape.

That is where the Federal government comes in, but instead of a strong Federal government that makes every effort to protect Americans' sensitive data, the Trump Administration and Department of Government Efficiency (DOGE) are dismantling our IT and cybersecurity workforce and replacing hardworking civil servants with unqualified hacks.

[Photo]

Mr. LYNCH. Just last week, President Trump installed a 22-year-old with no national security expertise to oversee a Department of Homeland Security hub for terrorist prevention. The Administration has spent the last five months weakening our leading cybersecurity and consumer protection agencies and purging the Federal watchdogs who ensure government works for the people's interests. I condemn those efforts, and if Committee Republicans were serious about this hearing, they would as well.

If we are concerned about the security and privacy of Americans' sensitive data, we need a hearing examining the myriad of ways that DOGE is violating cybersecurity and privacy laws, and making our personal information easier to steal or use against us. We need a hearing on how and why DOGE installed a server of unknown nature and origin at the Office of Personnel Management, or the specialized computers that DOGE engineers are reportedly creating to merge Americans' data across agencies with blatant disregard for Federal laws that ensure Americans know when their data is being accessed and by whom. We need a hearing on the way that DOGE has exposed critical Federal systems to hostile foreign actors, and on the massive cuts to its personnel that DOGE has made across the government, including at critical agencies like the Social Security Administration, which houses every American's Social Security number.

Last week, Republicans on the Committee voted against, again, to shield Elon Musk from accountability for the destruction and danger he has wrought on Americans, quite possibly under the influence of hard drugs, but this is the Oversight Committee and the American people deserve answers. We have weak privacy laws, persistent threats from foreign adversaries, and Trump's own estranged top advisor and a President who is both intentionally and through incompetence crippling the Federal government's cybersecurity defenses, privacy safeguards, and oversight capabilities. This perfect storm leaves Americans' sensitive data vulnerable to breaches, exploitation, and surveillance. Americans, not private companies, hackers, or Elon Musk and DOGE, deserve to own their data and make the decision about how, where, and if their sensitive information is used.

I hope my Republican colleagues will join us in taking a comprehensive approach to securing Americans' private data because while it appears Americans can opt out to delete their data from 23andMe, there are no options to delete their data from DOGE. Mr. Chairman, I yield back.

Chairman COMER. The gentleman yields back. I am pleased to introduce our witnesses. Today, all witnesses are testifying in their personal capacities.

First of all, Anne Wojcicki is a co-founder, board member, and former CEO of 23andMe. Before co-founding 23andMe, Ms.

Wojcicki worked at various hedge funds and investment companies as a healthcare analyst. She founded 23andMe in 2006. Ms. Wojcicki served as CEO of 23andMe for almost 20 years. Her service as CEO voluntarily came to an end on March 23, 2025.

Joe Selsavage is the current interim CEO of 23andMe as of March 23, 2025. He began working for 23andMe in November 2021 after the company was acquired by Lemonaid Health. He served as 23andMe's Chief Financial Officer as he has over 25 years of accounting and finance experience. He formerly worked as a consultant and chief financial officer for various companies. 23andMe's board chose Mr. Selsavage to serve as interim CEO after Ms. Wojcicki voluntarily resigned her resignation and 23andMe's simultaneous bankruptcy announcement on March 23.

Dr. Margaret Hu is the professor of law and Director of Digital Democracy Lab at William & Mary Law School. She previously served as special policy counsel in the Civil Rights Division of the U.S. Department of Justice.

Pursuant to Committee rule 9(g), the witnesses will please stand and raise their right hands.

Do you all solemnly swear to tell the truth, the whole truth, and nothing but the truth, so help you God?

[A chorus of ayes.]

Chairman COMER. Let the record show that the witnesses have answered in the affirmative. Thank you all. You may take a seat.

We appreciate you being here today and look forward to your testimony. Let me remind the witnesses that we have read your written statement and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes. As a reminder, please press the button on the microphone in front of you so that it is on and the Members can hear you. When you begin to speak, the light in front of you will turn green. After 4 minutes, the light will turn yellow. When the red light comes on, your 5 minutes have expired, and we would ask that you please wrap up.

I now recognize Ms. Wojcicki for her opening statement.

STATEMENT OF ANNE WOJCICKI, BOARD MEMBER, 23ANDME HOLDING CO.

Ms. WOJCICKI. Chair Comer, Ranking Member Lynch, and Members of the Committee, my name is Anne Wojcicki. I co-founded 23andMe nearly two decades ago with the mission of helping people access, understand, and benefit from the human genome. My personal mission is to have a meaningful impact on the world. It has been my life's passion to understand the human genome and DNA, the code of life.

The Committee has raised important questions about the protections and privacy that 23andMe applied to our customers' data. Over the company's almost 20-year history, these are questions we thought seriously and deeply about. We did this because our focus has always been on improving the health of our customers. If we did not have their trust, we would not have been able to do the groundbreaking research that impacted millions of lives.

Let me be very clear about our practices and what we stood for. During my time as CEO, privacy was central to every decision we made from product development to research initiatives. Customers

had choice and transparency about what information they saw and how they consented for their data to be used. Customers were required to give explicit consent before their anonymized data was used for any research purpose, and over 80 percent of our customers made the choice to opt in. We never provided information to any third party without the customer's explicit consent. With that foundation, let me turn to our mission and what we were able to accomplish for our customers.

The company's mission was driven by the belief that it is an individual's right to be able to affordably access their own genetic information and to learn what it means for them. This guiding light has always been at the core of 23andMe's mission and core to my beliefs. 23andMe pioneered the field of genetic ancestry and direct-to-consumer genetic testing. The journey of pioneering access to genetic information for individuals has not always been easy, but I am incredibly proud of the impact we have had. Over 15 million customers have learned about their ancestry, found relatives, and potentially lifesaving health information. For example, over a million customers learned they carried a genetic variant associated with blood clotting risk, allowing them to seek care to prevent potentially fatal clots. Customers also gained information about sickle cell disease, chronic kidney disease, type 2 diabetes, and coronary artery disease. In many cases, these reports were lifesaving. Hearing from customers about how their genetic information changed their lives is what drives me every single day.

One recent email from a customer read, "Hi Anne. I just wanted to share my story with you because I was diagnosed with breast cancer on June 24, 2024, at the age of 33. I had no symptoms at all, and the doctors felt no lumps. It was all because of 23andMe that I even got a mammogram, and because of that, we have caught it at an early stage. And although the upcoming months will be hard, it could have been so much worse. A few years ago, I did 23andMe and we did the health version, and it showed that I had the BRCA1 gene mutation. I have no family history that we know about, so I was not on track to get a mammogram until I was 40. I just wanted to send this testimony and say thank you. I am so indebted to you for making me aware of this, and I truly feel like because this was caught early, my life is saved and I owe you that. From me, my family, my friends, and my 1-year-old daughter, thank you for saving our lives."

Let me be clear. None of these discoveries that saved lives would have been possible without scientific research. During my tenure as CEO of 23andMe, our research program was truly groundbreaking. The impact of our research has extended far beyond our customers. It has benefited the broader scientific community and communities from coast to coast. When I spoke with customers facing serious health conditions, their message to us was clear: use the data we gave you. Help us if you can or help someone else. Do not store it. Do something with it.

With my remaining time, I want to address one last topic: China. The threat posed by China to the biotechnology sector is real and is not new. China has made massive investments in life sciences and biotechnology and is rapidly positioning itself as a global leader. Meanwhile, the U.S. is falling behind. This disparity concerns

me deeply. Understanding the human genome is not just about scientific advancement, it is about national security, global competitiveness, and the health of all Americans. This belief has fueled my work throughout my career, and it continues to drive my unwavering commitment to advancing genomics for the public good. As I believe you know, I am currently pursuing an acquisition of the company as an independent bidder during the bankruptcy proceedings. Looking forward, I remain committed to this mission in driving meaningful change in our healthcare system by continuing to empower individuals and enable them to make informed decisions about their health because the future of healthcare belongs to all of us.

I appreciate the opportunity to be here today, and I look forward to your questions.

Chairman COMER. Thank you very much. I now recognize Mr. Selsavage.

STATEMENT OF JOE SELSAVAGE, INTERIM CEO, 23ANDME HOLDING CO.

Mr. SELSAVAGE. Chairman Comer, Ranking Member Lynch, 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 a 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 customers by providing access to information about their personal genetics based on the latest science so that they can make 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 tendencies.

23andMe's customers have consistently reported taking positive health actions after learning about their genetics through 23andMe services. Eighty-two percent of our customers with actionable genetic results 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 for 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 tenant of 23andMe's research program. We have separate research consents beyond our consent to processing sensitive data, a privacy statement, and terms of service that customers must review and agree to separately if they want to participate in our research program. We remove all identifying information before any genetic data is shared with any third party. And any customer who affirmatively consents to participate in our research program can easily opt out at any time through their account settings and always have been able to do so. Customers are also free to delete their accounts and information at any time. 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 advocacy organizations, universities, and biotech companies to bring customer opportunities to participate in research. Since 2010, 23andMe has published 293 papers that helped 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 to the winning bidder is presented for the approval by the court. Because this proceeding is ongoing, I am unable to speak about the merits of either bid for the ongoing sale process, but let me assure the Committee that 23andMe remains committed to protecting customer data. We are requiring that anyone bidding for 23andMe must comply with all of our privacy policies. We recognize the vital importance of protecting every individual's right to access and control their 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 process.

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 the Committee today, and I welcome your questions.

Chairman COMER. Thank you very much. I now recognize Professor Hu for her opening statement.

STATEMENT OF MARGARET HU (MINORITY WITNESS), PROFESSOR OF LAW, WILLIAM & MARY LAW SCHOOL

Professor HU. Thank you. Good morning, Chairman Comer, Ranking Member Lynch, and Members of the Committee. I am Margaret Hu, Davison M. Douglas professor of law and Director of the Digital Democracy Lab at William & Mary Law School in Williamsburg, Virginia. Thank you for the opportunity to address the urgent matter of how best to secure Americans' genetic data privacy.

As this Committee recognizes, the collection, storage, and analysis of sensitive genetic information and its disclosure can pose a range of national security concerns and risks. The bankruptcy proceedings of 23andMe demonstrate why these matters are so consequential, especially in the age of artificial intelligence and the future of AI warfare. The first decade of my law career was dedicated to the Civil Rights Division of the U.S. Department of Justice. My first day as a trial attorney was the day before the terrorist attacks of September 11, 2001. I immediately joined a post-9/11 task force and focused on Homeland Security and border security issues. In the past decade, I have served as a researcher and a professor of AI law, constitutional law, and national security law. I would like to approach this topic from the perspective of AI and national security. My post-9/11 policy work introduced me to the topics that now form the basis of my current research in data privacy, cybersecurity, and AI governance with a particular focus on biometric cybersurveillance and biometric cyber intelligence.

This hearing is critically important. Genetic data and biometric cyber intelligence lies at the very center of a new battlefield in the age of AI. Safeguarding the genetic data of 23andMe and other biotech corporations is not just a matter of data privacy. It is of paramount importance as a matter of national security. Consequently, in addition to discussing the bankruptcy and consumer data protection laws of this current matter, I am grateful for this opportunity to support the Committee's examination of the national security implications of the sale and transfer of this sensitive data. The topic of genetic data privacy unfolding within the context of this bankruptcy proceeding is simultaneously unfolding within the context of a much larger crisis: inadequate Federal data privacy and cybersecurity safeguards generally and inadequate Federal laws to address the challenges of the AI revolution. The 23andMe bankruptcy filing is a wake-up call that our current legal inadequacy amounts to instability in our national security.

In the age of AI, data privacy, cybersecurity, and AI infrastructure form the tapestry of overlapping systems of law and technologies. The Federal Aviation Administration (FAA), for example, coordinates airspace and aircraft traffic control, aircraft safety and investigation, and sets standards for the National Airport Systems. Without question, the FAA is seen as an essential national security partner coordinating closely with the U.S. Department of Defense as it supports both civil and military aircrafts. Congress should now immediately enact both Federal data privacy laws and cybersecurity laws, and also take legislative action to enact Federal AI laws that anticipate these important national security threats that can be posed by inadequate AI regulations. The 23andMe bankruptcy matter provides a window into why Congress should step forward and enact these laws that are capable of creating a similar administrative oversight structure as the FAA, including regulations that acknowledge the need to coordinate national security concerns in the handling of sensitive data.

23andMe holds the genetic and personal data of over 15 million individuals, including predispositions to disease, ancestral background, and familial linkages. This data is not only personal and permanent, it is relational, making the stakes unusually high. Al-

most seven million consumers were exposed in a data breach of 23andMe in 2023. The company entered into a settlement agreement that involved a $30 million settlement. Now, in the moment of AI warfare, there is a highly sensitive genetic data black market where foreign adversaries are fighting to get this data for a wide range of reasons, including for strategic advantage, sometimes referred to as military identity dominance or for cyber intelligence purposes. Biometrics included often referred to as hard biometrics, fingerprints, iris scans, and palm prints, and DNA.

In the intelligence context, the national security risks and misuses and abuses of genetic data by foreign adversaries may include potential biological warfare risks, blackmail, and increased surveillance among other potential threats. The Pentagon has previously warned military personnel that DNA kits could pose a risk to national security. Other harms could potentially include abusing genetic data for isolating and discriminatory targeting, and potentially analyzing genetic data and aggregating biometric data and biographical data for the purposes of cognitive warfare.

Data privacy is not only a consumer data privacy issue, but also a national security one. Thank you, and I look forward to your questions today.

Chairman COMER. Thank you very much, and we will now begin with our questions. I recognize myself for 5 minutes.

And Ms. Wojcicki, I really appreciate your opening statement and the fact that your company can identify the potential risk for cancer and things like that. I mean, that is great. But let us talk about—our concern is the national security risk of what happens with the data and how it can be used against consumers, and we are very concerned about that because there is a precedence here where companies with Chinese influence have stolen data. So, just to start off, with 23andMe, people provide a saliva sample to the company. What tests are run on the sample?

Ms. WOJCICKI. I appreciate the question. The test that was run, it was actually run on a gene chip that Illumina created. So, the sample was sent. Somebody takes a saliva sample. They get a tube.

Chairman COMER. Okay. Okay. So, what type of information did 23andMe obtain from the sample?

Ms. WOJCICKI. It was about 600,000 specific markers in your genome, so markers that are known to vary between humans known as snips.

Chairman COMER. Okay. So, are the samples tested? They are obviously tested for genetic markers, correct?

Ms. WOJCICKI. Correct. Correct. So, it was 600,000 genetic markers.

Chairman COMER. What is the purpose of testing the samples for genetic markers? Can you explain that?

Ms. WOJCICKI. Yes. The purpose for it was really twofold. It lets people have the opportunity to learn about their ancestry, where they are from in the world, potentially areas that they did not know about. They have the opportunity to connect with family members, potentially, for instance, adoptees who are looking to identify, you know, biological siblings or parents.

Chairman COMER. Right. Out of curiosity, is this optional for consumers?

Ms. WOJCICKI. It is completely optional because we realized there was a number of people who do not want to find additional family members, and that they did not want to be identified. So, it is an explicit consent where we ask people specifically, do you want to find close family members or distant and you have the ability at any time to toggle in or to toggle out of that. It is very easy to do.

Chairman COMER. So, did 23andMe also track genetic markers over time in order to conduct long-term health studies?

Ms. WOJCICKI. We did. So, we also specifically tested on markers that are known to be predispositions for health conditions. So, in my testimony, for example, I talked about the BRCA1. We specifically identified that there were a number of people who were not able to get their BRCA results because of the barriers that the insurance industry or their societies have put up. So, we found actually about 20 to 30 percent of our customers were learning that they had potentially, like, a really detrimental genetic variant that put them at very high breast cancer risk and they could not otherwise get that information.

Chairman COMER. So, you used this type of testing during COVID–19. What was the purpose of that?

Ms. WOJCICKI. Well, it was the same test that we started with in 2006. It was the same test going forward. We were very consistent.

Chairman COMER. What were the results?

Ms. WOJCICKI. It was the same. It was the same types of results.

Chairman COMER. Where did the data information from DNA swabs go once testing was complete?

Ms. WOJCICKI. So, we worked with Labcorp. Labcorp had been our partner for 18 years or so, so, it went to Labcorp. They have an office in LA as well as in North Carolina.

Chairman COMER. So, did the data get uploaded to a database?

Ms. WOJCICKI. Yes. So, they would then send us data files and that data would come into 23andMe. We also upload it. We work with Amazon, AWS, all on U.S. servers.

Chairman COMER. How was the data protected?

Ms. WOJCICKI. It was encrypted from end to end. We had all kinds of ways that, again, the team thought about how it was going to be encrypted, how it was sent. It also, I should be super clear, had no identifiable information when it was sent to Labcorp or when we received it, so we——

Chairman COMER. How long does the data stay in that database? How long? Forever?

Ms. WOJCICKI. At the 23andMe database?

Chairman COMER. I am sorry?

Ms. WOJCICKI. At 23andMe you mean?

Chairman COMER. Yes.

Ms. WOJCICKI. As long as the customer wants.

Chairman COMER. Or anywhere, how long does the data stay in the database?

Ms. WOJCICKI. As long as the customer wants. They have that opportunity to delete their data at any time.

Chairman COMER. So, where did the physical saliva sample go after testing is complete?

Ms. WOJCICKI. The physical saliva sample would go to Labcorp, and customers had the ability to say do I want my saliva sample stored or not stored. And the reason why they might want it stored is, for example, we were offering, in the future, potentially you would want to upgrade, you would potentially want to get a different type of test, or if there were additional services. So, we offered biobank.

Chairman COMER. If it was not stored, what happened? Did it get——

Ms. WOJCICKI. It was discarded.

Chairman COMER. It was discarded?

Ms. WOJCICKI. Correct.

Chairman COMER. You are sure?

Ms. WOJCICKI. We are sure.

Chairman COMER. Okay. Was it possible to run multiple tests on one sample?

Ms. WOJCICKI. It was possible to run multiple tests on one sample.

Chairman COMER. Okay. The last question. Under your leadership, did 23andMe scientists ever run multiple tests on a single sample, and if so, were customers notified about the additional tests?

Ms. WOJCICKI. We ran additional tests potentially for the FDA submissions that we did. So, in order to do validation studies, we would find customers with potentially very rare variants, and we had to do an additional type of test, sometimes called Sanger sequencing, to prove to the FDA that the results we were generating were indeed accurate.

Chairman COMER. Okay.

Ms. WOJCICKI. So, let me also be clear, we also sometimes did additional research studies. So, we would occasionally look and say let us do whole genome analysis for additional research studies.

Chairman COMER. Okay. Thank you. The Chair recognizes the Ranking Member.

Mr. LYNCH. Thank you, Mr. Chairman. Ms. Wojcicki, right?

Ms. WOJCICKI. It is Wojcicki, correct. Yes.

Mr. LYNCH. In my neighborhood, we have a Polish triangle where all the Polish families live. You look familiar.

Ms. WOJCICKI. Okay.

Mr. LYNCH. First of all, I appreciate you sharing your personal history here. And you know, I fully appreciate the value of early detection through 23andMe and other technologies as well in terms of the value that that provides for early treatment protocols for breast cancer. That is really, really, really important. I hope that is something that people get from this hearing today, but also your experience and your situation actually amplifies the need for greater privacy protections, right?

On this Committee, back in 2015—I was a Member then—we had a huge hack of the OPM servers, the Office of Personnel Management. So, the massive data breach back then compromised the personal information of about 22 million people, but most importantly, that included Federal employees and anyone in the Federal government that was applying for a national security clearance. So, think about that. In our government, who would need national se-

curity clearance, right? Those people who are doing very sensitive work, so all that information went over to the Chinese. It was a Chinese threat actor.

At that time, the Oversight Republicans, really, I have to give him great credit. Jason Chaffetz was the Chair of the Committee at that point. I was just a Subcommittee Ranking Member at that point, but we conducted an investigation, and they came up with 13 recommendations that the OPM system and its chief information officer should be empowered, accountable, competent, and should "improve Federal recruitment, training, and retention of Federal cybersecurity specialists." What the Trump Administration has done, though, is just done a blanket firing of some of our most talented cybersecurity experts. They have disregarded the cybersecurity and data privacy laws. DOGE is reportedly creating a master database of sensitive information across Federal agencies by carrying around unsecured backpacks full of laptops, paving the way for unparalleled surveillance capabilities. So, this is an extreme danger to the very systems that we want to protect.

So, Professor Hu, does firing all these IT and cybersecurity experts, does that make Americans' data safer?

Professor HU. Thank you for that question. I think that this raises deep concerns as far as how best do we safeguard very sensitive governmental data. And as you mentioned, the leadership of this Committee after the OPM hack, I think, was very important, not only in recommending best practices for cybersecurity moving forward for the Federal government, but also uncovering the ways in which the laws of this body, Congress, were not followed. And that some of those threats that created, the types of issues that we saw after the OPM hack could have been avoided.

And so, part of what we have seen over the last ten years is that the Federal government has undertaken very serious protocols and training programs and the hiring of some of the most qualified cybersecurity officials in these agencies. And now the concern is, once those are dismantled, the expertise and also the failure to follow the protocols that followed after the OPM hack, that that leaves our Nation's most sensitive databases and data on our citizens up to potential abuse and national security risks.

Mr. LYNCH. Let me ask you this. So, in the past we have several government agencies that collect troves of information. You think about Social Security, a lot of information about, you know, people getting benefits, their banking information, things like that. The census, you know, that is a repeat every 10-year process, we actually send people to folks doors to get personal information. The IRS, when you take a look at your tax return, you figure out all the information that you are giving the Federal government. We have kept those silos separate until now. Now, Elon Musk is joining those so all that information will be in one central database. We got that from a whistleblower. What kind of damage would that do to our national security and privacy?

Professor HU. Well, as was pointed out in the Oversight Committee hearing recently, especially by the testimony that we saw by Bruce Schneier, that the firewalls that are created by keeping those data decentralization creates additional security safeguards. And so, allowing for the integration and consolidation of that data

increases vulnerabilities in cybersecurity. It is much easier to create the types of risks of exposure that now are the heart of the topic of the discussion today.

Mr. LYNCH. Thank you. Mr. Chairman, I thank you for your courtesy and I yield back.

Chairman COMER. The gentleman yields back. The Chair now recognizes Dr. Gosar for 5 minutes.

Mr. GOSAR. Thank you, Mr. Chairman. As a former dentist, I know how important HIPAA compliance is for the doctor-patient trust. When customers sign up for testing like 23andMe, they pay for the service, not the storage, and continued research of their DNA, but at the minimum, American data should not leave American hands. China has already said it wants to create a database of genetic data to build bioweapons. If we are questioning whether our adversaries are going to use this genetic data to create a bioweapon against Americans, then quite frankly, this data collected from Americans should be destroyed, not stored.

Mr. Selsavage, how does 23andMe store customer's data? Is it physical or digital, or both?

Mr. SELSAVAGE. Congressman, it is both. I mean, 23andMe stores the digital data, and as Ms. Wojcicki mentioned and I did in my statement, security and data privacy is a top priority for the company. All of that data is stored in an encrypted format, and if customers do choose to biobank their sample, with a consent, the physical saliva sample is maintained as well.

Mr. GOSAR. Okay. So, when a customer requests their data to be erased, what kind of data is erased?

Mr. SELSAVAGE. All of the data that they have in the digital format, with the exception, you know, of their name, email address, and purchase information, is erased from the company's data records. In addition, if they had consented to biobank their sample, that physical sample is also destroyed.

Mr. GOSAR. So, now, in 2019, the Department of Defense advised our service members to avoid these types of DNA kits due to the security concerns. Can you address that? Why that would be?

Mr. SELSAVAGE. I am not familiar with, you know, why they requested that service members not do the personal DNA test.

Mr. GOSAR. So, let me ask you the next question. Have you ever participated in a 23andMe test? Is your data at risk, too?

Mr. SELSAVAGE. My data is at risk. I first joined 23andMe in 2013 and have done subsequent tests with new health chips with 2013 and have continued to maintain my personal data and have not deleted it, and I continue to biobank my sample with 23andMe.

Mr. GOSAR. Ms. Wojcicki. Did I say it wrong?

Ms. WOJCICKI. No worries.

Mr. GOSAR. Okay.

Ms. WOJCICKI. That is perfect.

Mr. GOSAR. I tell everybody I speak two languages, one not so good and that one is English. So, as a former CEO and board member of 23andMe, do you have access to the customer's data?

Ms. WOJCICKI. I do not.

Mr. GOSAR. Who would be accessible to that data? Who could get to that data?

Ms. WOJCICKI. That is a great question, and as I mentioned before, privacy and data security was always top of mind when I was CEO at 23andMe. So, we came up with very strict protocols about how you could ever link up genetic information with the identifiable information. So, if you think about how our databases were set up, all of your personal information, meaning your name, your address, your email, was in a separate database that was stored separately. Very few people could connect it then with the genetic information, so from a database design, it was separated out.

So, a few people within the company had the ability to put that key together. So, for example, imagine if you were a customer and you did not get the right results, or you have a question about something, or you are wondering, something does not make sense to you. You would have to be able to call the customer care team and they would have to be able to analyze your results, so only in very specific situations would we ever be able to reconnect that. And so, I should also be clear, when we did research identifiable information, like your name, your address, your email, was never part of that, and none of the partners that we ever had, had any identifiable information.

Mr. GOSAR. So, when I see a data like this, a "Hacker has got nearly seven million people's data from 23andMe, the firm blamed users in a very dumb move." I want you to put this to the record. Could you address this?

Ms. WOJCICKI. Yes. So, the situation that happened there, and we have said before to our customers and everything that happened, that there was a deep apology for everything that has happened here. It was a credential stuffing, so it was not actually a breach of our systems. It was credential stuffing, and what that actually means is that the threat actor found old addresses, email addresses and passwords, on the dark web, and they ran them against 23andMe, and they found a number of customers where they actually could enter into their accounts, so it was specific. It was a credential stuffing incident, and through that, they were able to actually get access to their account.

Since then, we have made pretty substantial changes. So, in response, we immediately wanted to learn from this, so we forced all of our customers to reset their password, so every single customer had to go and reset their password. And then second, we had double-factor authentication, which was mandated, and we had actually had two-factor authentication for a while, but it was not mandated because it was not industry standard.

Mr. GOSAR. Thank you, Mr. Chairman. I yield back.

Chairman COMER. The Chair recognizes Ms. Norton from Washington, D.C.

Ms. NORTON. Thank you, Mr. Chairman. When Elon Musk joined the Trump Administration, he reportedly described himself as "tech support" for the Federal government. Clad in an absurd "tech support" tee shirt, Elon Musk assured President Trump's Cabinet that slashing the Federal workforce was necessary to save the Federal government money and make it more efficient. We all saw what happened next. The so-called Department of Government Efficiency threw the government into chaos by recklessly firing Federal employees regardless of their role, experience, or their value brought

to the agencies. This effort has ultimately cost taxpayers more than $135 billion, according to Partnership for Public Service.

The Trump Administration's purge of the Federal workforce is also making it harder for the government to maintain its sensitive databases and records and prevent cyberattacks. The U.S. Digital Service was the technology office in the White House that led modernization of Federal technology and software systems, that is until the Trump Administration. Then Elon Musk took over and fired dozens of its employees. Another 21 IT workers resigned from the office rather than carry out the destruction Musk demanded of them. The mass resignation letter signed by these skilled engineers, data scientists, and IT professionals, included a stark indictment of the Trump Administration, explaining that they had been asked to take actions inconsistent with their oath to serve the American people and uphold the Constitution.

I ask unanimous consent to enter this letter into the record, Mr. Chairman.

Chairman COMER. Without objection, so ordered.

Ms. NORTON. The U.S. Digital Service is not only the only Agency that has been gutted. IT personnel have been laid off across the Federal government, leaving many agencies further exposed to threats. For example, the Department of Government Efficiency demanded a 50-percent cut in the technology division of the Social Security Administration. This division maintains the Social Security Administration's website, benefits, portals, and IT systems. The Trump Administration also reportedly planned to fire an additional 25 percent of the employees who manage the data systems at the Social Security Administration. Professor, how has the Trump Administration's purge of IT and cyber professionals left the Federal government more vulnerable to data intrusions?

Professor HU. Thank you for that question, Congresswoman. I think that what we are witnessing, especially in news reports with DOGE now entering into 17 agencies and the dozens of lawsuits that have followed since the start of DOGE, is a deep concern about whether or not this falls outside the scope of what is constitutional or legal, particularly given this body. The Digital Services Office that you referred to was something that received funding and was specifically included legislatively, is my understanding, whereas DOGE is not, and that is part of the current litigation, whether or not this type of body is legal, is constitutional, and whether or not these types of actions that you describe are also outside the scope of the law both with FSMA, for example, and the Administrative Procedure Act. So, we just saw within the last couple days, you know, in the district court a concern about the OPM databases and whether or not an injunction is necessary in order to stop continued access.

Ms. NORTON. The Trump Administration's proposed 2026 IRS budget would cut a staggering $8 billion and nearly 20 percent of positions from fiscal 2025 levels, including 60 percent of the IT staff. Professor, what are the risks of making a massive cut to the IT workforce at the IRS, which holds the most sensitive financial information of every American?

Professor HU. Thank you for that question. The attempt to consolidate the information that is so sensitive—our financial informa-

tion, our tax information, our information about our health—in order to try to create that type of consolidation increases the national security risk tremendously. As we saw from the OPM hack, for example, that you had millions of Americans' data exposed, but not only their biographic information, but their biometric information. So, as a result of the 2015 hack, it was reported that 5.6 million fingerprints were also then released. So, these are very serious issues, particularly with national security implications.

Chairman COMER. Thank you. The gentlelady's time has expired. The Chair recognizes Dr. Foxx from North Carolina.

Ms. FOXX. Thank you, Mr. Chairman and thank you to our witnesses for being here.

Mr. Selsavage, we all know the Chinese Communist Party has a track record of misusing genetic data, and even the *New York Times* acknowledged that "China used its genetic tests to track members of the Uyghur," who are a politically disfavored minority group. This abuse can surely be perpetrated against any disfavored group whose genetic data is available. How does 23andMe prevent the genetic data, mainly from Americans controlled by the company, from being used by the CCP or some other malign actor to track or harm Americans?

Mr. SELSAVAGE. Congresswoman, you know, 23andMe puts data security and privacy at the top of the forefront of our company. You know, all of our data is secured with top security encryption. You know, we have, you know, security professionals in place at 23andMe implementing the latest technologies in security, and we have received three ISO certifications for the company in terms of security, cybersecurity, and privacy to make sure that the data of our customers is secure.

In addition, after the cybersecurity incident, we made sure that, you know, basically we have implemented two-factor authentication. We have ensured that customers have reset their passwords, and we make sure that those passwords have not been, you know, basically in the compromised databases anywhere to make sure that our customer data is safe.

Ms. FOXX. Mr. Selsavage, besides the 15 million individuals who have their genetic data stored with the company, family members, by virtue of having a similar genetic makeup to those who took the test, are also potentially at risk if 23andMe's genetic data is exposed or used for nefarious purposes. Is that correct?

Mr. SELSAVAGE. You know, if a customer at 23andMe chooses to allow their data to be shared, such as a DNA relatives feature at 23andMe, you know, relatives could actually and family members can see that additional data, yes.

Ms. FOXX. Ms. Wojcicki, precisely because of concerns about the genetic information controlled by 23andMe falling into the wrong hands, the Pentagon warned its personnel in 2019 not to use consumer DNA kits. How did 23andMe respond to the Pentagon's warning at that time?

Ms. WOJCICKI. Thank you for that question. I have to say, in all honesty, we were surprised. We had not been contacted. We were surprised. So, we were happy to engage around that discussion as to what are the potential concerns, but it was a surprise to us, and

we did not get forewarning and we did not know and engaged afterwards.

Ms. FOXX. So, after the warning, did the company change the way it handled or protected consumers' genetic data?

Ms. WOJCICKI. Thank you for that. There were not substantial changes because, as I mentioned, privacy and data security had really been top priority since the inception of the company. So, I would say after that notice and reading about that, it definitely became top of mind, and I think the number one takeaway we had was, really, there should be an engagement around the understanding of how we actually are making sure that we are securing data and how we are making sure that customers, we are always honoring the customer's privacy. So, it was a great opportunity for us to consider engaging. We always are reviewing our systems. We are always looking at sort of the update of what else should we be doing with our security protocols, and so that was the primary takeaway from that.

Ms. FOXX. Do you believe there is anything that could have been done to prevent the 2023 breach?

Ms. WOJCICKI. I appreciate that question. I am pretty limited with what I can say specifically around that because of the potential litigation or the ongoing litigation around there. The thing that we always said, is that you have to be vigilant on a daily basis. You have to always live in a world of paranoia because you see how many threat actors there are out there, the number of security incidents that are there. So, the primary takeaway we always thought is like, what is also the product by design? How are we making sure we are designing the product so if and when something happens, that we are doing everything we can to protect the privacy of our customers. The database security design has always been really important for us about making sure that if there ever was a threat actor, how are we actually making sure that we are doing everything we can to prevent that. So, it was always top of mind for us to think about what those potential risks are.

Ms. FOXX. Thank you. Mr. Chairman, I yield back.

Chairman COMER. The gentlelady yields back. The Chair recognizes Ms. Brown from Ohio.

Ms. BROWN. Thank you, Mr. Chairman. Today's hearing gives us an opportunity to explore bipartisan solutions to protect Americans' personal identifiable information. When services like 23andMe first launched, they were seen as groundbreaking, giving people unprecedented access to information about their ancestry, health, and genetics. For the first time, you could uncover long lost family connections or gain insights into potential health risks all from the comfort of your home. But what many of 23andMe's nearly 25 million customers did not realize was that unless they actively opted out, they were also consenting to share their personal DNA data with third parties. Unlike a password, you cannot change your DNA, and it cannot truly be anonymized. What is more, one person's genetic data can reveal information about their entire family. Now with that company's future uncertain, the safety and security of that data hangs in the balance. Americans deserve real oversight and tough privacy protections to keep their most sensitive data safe.

Mr. Selsavage, when you became the CEO just as 23andMe experienced a massive breach that exposed the sensitive genetic data of seven million users, what concrete steps have you taken since to prevent this from happening again? And what can you tell your customers today, right now, that you could not say a year ago to reassure them their most personal data is safe?

Mr. SELSAVAGE. Congresswoman, you know, I want to reiterate that 23andMe always has put our consumers' security, data security, and privacy at the forefront of the company. Since the data incident, we have implemented additional security measures. We, you know, force every customer to actually reset their password to make sure that their accounts are safer. We implemented two-factor authentication, whereby a customer either gets an SMS or an email sort of code to actually enter in addition to their password to make sure their data is secure. And then we also ensure that any sensitive data, like the personal genomic data that the customer has, if they requested that data, that there was additional verification of the customer requesting it, such as their date of birth and other credentials, and then also put a time limit so that they could not access that data immediately, but rather put a time delay of 48 hours on that data.

In addition, we have hired a new chief information security officer at the company and put in additional security controls. Through the bankruptcy process, we are making sure that, essentially, through the process, that our customers' data is safe because we are requiring any bidder for the company to continue with the privacy policies and consents that are in place here at 23andMe.

Ms. BROWN. Thank you. We are having this conversation at a time when foreign adversaries, like China and Russia, are working overtime to exploit Americans' personal data. We know that China has targeted Americans' genetic data to train their AI technologies to develop advanced medicine and even for military research, and we are facing this threat with fewer resources. The Trump Administration has made massive cuts to funding and staffing at our Nation's top cybersecurity agencies. We need both strong cybersecurity protections and Federal privacy laws to protect Americans' data. So, Ms. Hu, as you know, there is no Federal framework for how private companies handle consumer biological data. What steps should Congress take to ensure that private industries is not putting Americans' private health and genetic data at risk, especially in the hands of our foreign adversaries?

Professor HU. Thank you so much, Congresswoman, for that question. I do believe that we need an overlapping regime that takes into account both strong Federal data privacy protections that now need to update laws such as HIPAA, that do not cover these types of new biotech services and wearables and other types of apps. New health data is being generated that is not covered under our existing health data protection laws, and we are increasingly faced with cybersecurity laws and data privacy laws at the state level that are now stepping in to fill the gap that is being left by Congress, but especially, with AI warfare on the horizon, it is absolutely critical. And I agree with you, this is a bipartisan issue.

Ms. BROWN. Thank you so much. I will close with this. Americans deserve to know their sensitive private data is safe and se-

cure. I look forward to working with my colleagues on both sides of the aisle as we continue these important conversations, and with that, Mr. Chairman, I yield back.

Chairman COMER. Thank you very much. The Chair recognizes Mr. Palmer from Alabama.

Mr. PALMER. Thank you, Mr. Chairman. Ms. Wojcicki, you initially shared data with GlaxoSmithKline (GSK) in regard to research on Parkinson's, and then in 2023, it looks like you shared the entire database with them. Is that correct?

Ms. WOJCICKI. I appreciate that question. In 2018, we——

Mr. PALMER. I need "yes" or "no." Did you share the entire database?

Ms. WOJCICKI. No, what we did was share specifically. The partnership was around using genetic insights for drug discovery, so we specifically use not the entire data set, but what we did is we analyze it. We are looking at all the genetic information we have, phenotypes like Parkinson's and saying, what is it? What is that genetic association?

Mr. PALMER. But you received an additional $20 million, and I think at that point, you are realizing that the company was in financial trouble. And it looks to me like you made a decision to provide more than what you had provided earlier, but you also said that people had the opportunity to opt out of that. How aggressive were you in notifying your customers that they had the opportunity to opt out of that data being shared with GlaxoSmithKline?

Ms. WOJCICKI. Yes. I appreciate the question.

Mr. PALMER. Were you aggressive, not that aggressive? Was it an email notification? How aggressive were you? Did you try to make sure that they understood they could opt out?

Ms. WOJCICKI. We actually sent an email notification to all of our customers at the time of the signing of the GSK collaboration with a link.

Mr. PALMER. Did you receive a follow-up from people who later found out the data had been shared that they wanted to opt out, but they did not do so before you shared the data?

Ms. WOJCICKI. Customers always have the opportunity at any time to opt out, so some number of customers did respond to that email. They opted out.

Mr. PALMER. When they opted out, does that include removing the data from GlaxoSmithKline?

Ms. WOJCICKI. It removed the data from all future analyses.

Mr. PALMER. But I am asking now, if you were not very aggressive in notifying people before you shared it with the pharmaceutical company, and people found out later that it had been shared and they wanted to opt out, was their data removed from GlaxoSmithKline?

Ms. WOJCICKI. Their data would have been removed from any future GlaxoSmithKline——

Mr. PALMER. Yes, you are saying "any future," but any past sharing of their data, you are saying that it is pretty much gone?

Ms. WOJCICKI. It was never individual's data. It was the aggregate. So, essentially, it is the summary. It is the analysis, so saying this specific gene is associated with Parkinson's.

Mr. PALMER. Let me ask you this. When 23andMe publicly announced it was filing for bankruptcy, roughly how many users reached out to 23andMe to delete their account and their data altogether?

Ms. WOJCICKI. I was not part of the company at the time, so I would not be able to answer.

Mr. PALMER. Mr. Selsavage, can you answer that?

Mr. SELSAVAGE. Yes, I can. From the time we actually announced bankruptcy until today, approximately 1.9 million customers have requested that their——

Mr. PALMER. Well, that is what?

Mr. SELSAVAGE. Roughly 15 percent.

Mr. PALMER. Fifteen percent. If a user wanted to delete completely their entire account with 23andMe and delete all of their identifying data, does 23andMe allow that, and if so, what does the process look like? I really do not want to know what the process looks like. I just want to know if they have the ability to do that.

Mr. SELSAVAGE. The customer has the ability to do that, and for any customer, it is a very easy process. They can just log into their account, go to their settings, and request their account and data be deleted.

Mr. PALMER. 23andMe became popular because you advertised it as identifying familial connections that go back centuries in some cases. How accurate would you say that data is?

Mr. SELSAVAGE. You know, for our DNA relatives feature, you know, we believe that those features are highly accurate, and, essentially, we actually take a look——

Mr. PALMER. When you say, "highly accurate," could you put a percentage on that? Is it 100 percent accurate, 90, 80?

Mr. SELSAVAGE. You know, it is in the high 90s percent of accuracy.

Mr. PALMER. High 90s? The thing that concerns me here is how you advertise your product, and I am not sure that people understood that you were planning to share that data with other companies because once they share their DNA sample with you, that is a one-time sale. There is no repeat business from that. You have to generate income from other means, and, apparently, you did that through sharing that data with pharmaceutical companies.

Let me ask you this. Do you support the motion filed by 27 state attorneys general to request the bankruptcy court appoint a consumer privacy ombudsman and a security examiner? Do you support that?

Mr. SELSAVAGE. Congressman, yes, respectfully. The company was first to actually——

Mr. PALMER. Very quickly. I got a last question.

Mr. SELSAVAGE. Yes, we support that. Yes.

Mr. PALMER. Has a 23andMe employee ever had access to the data, other than those who are cleared to have it? Has anybody else ever had access to that data?

Mr. SELSAVAGE. To the best of my knowledge, only people with the need to access that genetic data at 23andMe have access to it.

Mr. PALMER. That is to the best of your knowledge, but you cannot assert that no one else has had access?

Mr. SELSAVAGE. Congressman, that is to the best of my knowledge. As indicated, I have only been interim CEO since March 2025, but to the best of my knowledge, no other individual other than the employees who have a need to have access to data have had access to it.

Mr. PALMER. Mr. Chairman?

Chairman COMER. Yes, sir.

Mr. PALMER. I think we need a more certain answer on this about who has had access to this data. I see Mr. Lynch is in agreement.

Chairman COMER. Absolutely.

Mr. PALMER. So, could you do a deep dive investigation to make that determination, notify the Committee through Mr. Chairman and the Ranking Member?

Mr. SELSAVAGE. Congressman, I will take that back to our team and look into that for you.

Mr. PALMER. That is not a look into. That is a required reply.

Mr. SELSAVAGE. That is understood. We will take that back.

Mr. PALMER. Thank you, sir. I yield back.

Chairman COMER. Thank you. The Chair recognizes Ms. Stansbury from New Mexico.

Ms. STANSBURY. Thank you, Mr. Chairman, and thank you to our witnesses for being here today. This topic is of particular interest, I think, not only to myself, but millions of Americans, not just because the company in question here actually owns the genetic data of millions and millions of Americans, but because of what is happening right now with DOGE, with the Trump Administration, with private contractors getting multi-million dollar contracts to integrate Americans' personal data, with the court cases that are in front of the Supreme Court and the district courts, and this proposal that came through this House just two weeks ago in the dead of night that basically would preempt state and local laws from regulating our private data through AI systems.

And so, I mean, it is hard to not sit here and listen to this conversation and not feel like we are living through a sci-fi movie, right? Like we have all seen this scary sci-fi movie before that our private biological data—not me personally; I am too much of a privacy freak to do these genetic tests myself—that a private company has our data, they experience bankruptcy, and now we have no Federal regulatory system to protect that data, and we are concerned that foreign adversaries might purchase the company and thus the data. I mean, this is insane. This is crazy.

And meanwhile, I completely agree, this is bipartisan in this hearing, but our colleagues across the aisle are trying to pass legislation that would deregulate and preempt data privacy and AI laws across the United States in every single state and locality for the next ten years. That is bonkers. Like, you cannot have it both ways. You cannot haul a private company in before Congress to talk about their bankruptcy and the fact that they had 15 million Americans' private biological data and you want to protect it, and then you are trying to use Congress to preempt state and local law so that we cannot protect private data. Like, that is completely intellectually incongruent and dangerous for Americans.

Professor Hu, I was really interested in your background because you have worked both on the DOJ side as well as on the academic side. And you have outlined some of this in your testimony, but I am particularly interested in your background in national security and prosecuting national security cases. And if you could talk a bit more about this, like, political intersection we are seeing right now in this moment and what threats that poses for not just national security with foreign adversaries, but the potential that Americans' data could be misused by private companies here in the United States.

Professor HU. Thank you so much, Congresswoman. I think because of the bipartisan nature of this topic, it is so critical to come together and try to advocate for the types of legal framework that we need in order to address these national security threats appropriately. And I do believe that part of the issue right now is because in an absence of congressional legislation, we are asking these corporations to come in and fill that gap. And so, we are asking of companies, like 23andMe, you need to have the best data privacy, the best cyber security possible, but what about Federal law that then mandates that instead of looking to industry standards?

And I am very concerned about the moratorium and the idea that in the absence of Federal law that regulates comprehensively AI systems, that we would ban and bar states and localities from going forward with their attempts to try to offer some type of meaningful safeguard on these types of technologies. And so, thank you very much. I do think that this is so critical for there to be true bipartisanship for this national security issue.

Ms. STANSBURY. Thank you, and, you know, one of the things I really want to emphasize, for folks who are out there watching this and concerned about data privacy, which I believe is everybody. You know, I watch my share of both liberal and conservative news, and, I mean, everybody from Theo Vaughn to our colleague Marjorie Taylor Greene to myself to this side of the aisle are raising the alarm on this provision because of the significance that it has for the safety of Americans.

And so I think it is really, really important that we elevate this conversation right now and understand what they are proposing in this bill because when you read that bill, it literally not only says we would preempt state and local laws, it basically says any company even that wants to use an AI system in a locality could not be barred from accessing your data, which means that, presumably, a private company that does not have privacy and secured data systems could then be compelled under this preemption law to give away your data. I mean, that is dangerous. That is dangerous. So, I really appreciate you all being here today and we are going to continue to work on this issue. Thank you, Mr. Chairman.

Chairman COMER. Thank you. The Chair now recognizes Mr. Grothman from Wisconsin.

Mr. GROTHMAN. Yes. Ms. Hu, first of all, just kind of a big picture thing here, if these guys have my genetic data, why should I care?

Professor HU. Genetic data is and biometric data is now increasingly anchoring modern warfare because of the attempts in AI-driven targeting to try to aggregate biographic and biometric data. And

so, part of what I think is misunderstood is that this is not really a consumer data privacy issue alone, that this really does map into very significantly the way in which we conduct national security strategies.

Mr. GROTHMAN. Okay. So, I should be afraid that if we go to war—well, I hope we never go to war—if we go to war and they know my genome, that they will find some way to target me.

Professor HU. Well, it is not just an active, kinetic type of warfare situation. The new battlefield of AI warfare is really engaged in cognitive security issues and also the way in which we look at manipulation, social engineering as a cybersecurity risk.

Mr. GROTHMAN. Okay. Give me an example.

Professor HU. So, the way in which, for example, if we go back to the OPM hack of 2015 occurred, many experts say that it was through social engineering, that the way in which the Chinese hackers got access into the OPM systems was through social engineering, some type of manipulation. And so, at first, that they were able to manipulate somebody within OPM to give up their passwords, and then from there, able to install this type of——

Mr. GROTHMAN. How would they manipulate them?

Professor HU. Well, one of the examples given by some cybersecurity companies were the ways in which Chinese would pose, for example, as trying to present some type of alumni event from your university, and to get you to click on that, and then to install the malware from there.

Mr. GROTHMAN. Because they have my genome?

Professor HU. Well, the fact that the Department of Defense raised the alarm about the potential risks of it, I think, are really important for us to examine why. Why is the Department of Defense saying that this should not be something that the military should access? And I think it is——

Mr. GROTHMAN. Okay. I can think of reasons that is of concern, but not exactly your reasons. I will take it, though, for granted that we do not want to have my genome out there on the internet floating around. Mr. Selsavage, if I could use this company's services in the past, where is my data kept right now?

Mr. SELSAVAGE. The actual data and, basically, this data is stored on Amazon Web Services in secure, encrypted database files.

Mr. GROTHMAN. And can we assume that my data will be there after I die or right now, under the current law, be there forever?

Mr. SELSAVAGE. Your data is there, but you always have the right to delete your data at any time, and your beneficiaries and executors of your will or trust will also have the right to delete that data in the future.

Mr. GROTHMAN. Does anybody call right now to have their data deleted?

Mr. SELSAVAGE. Yes. Since we announced bankruptcy, we have had 1.9 million customers called and requested that we delete their data, and we have done so within a reasonable timeframe.

Mr. GROTHMAN. How many customers called to delete their data?

Mr. SELSAVAGE. Called or emailed or requested their data be deleted, there was 1.9 million customers.

Mr. GROTHMAN. That is kind of amazing, I think. I mean, I think it is probably a smart thing to do, but it would not occur to me.

Okay. Next question. Does Regeneron intend to update their privacy policy?

Mr. SELSAVAGE. Regeneron and TTAM Research Institute, both of the bidders under the current bankruptcy rules for the bidding process for the company, have both agreed to maintain the privacy policies and consents of the company of 23andMe in the future.

Mr. GROTHMAN. So, by that, you mean they are not going to change anything? They are saying they are not going to change anything?

Mr. SELSAVAGE. Not only did they say they are not going to change anything, they also agreed to that in their contract, which is an asset purchase agreement, in writing that they would continue to maintain the policies.

Mr. GROTHMAN. Okay. Ms. Wojcicki, are you aware that in 2015, 23andMe received $115 million in funding from a variety of investors, including WuXi Healthcare?

Ms. WOJCICKI. I am aware.

Mr. GROTHMAN. Okay. And you know they had ties with CCP?

Ms. WOJCICKI. I have been made aware of that, yes.

Mr. GROTHMAN. Okay. Did you consider this a risk at all, or do you think, for you or in the future, anybody should care that the Chinese take over one of these companies?

Ms. WOJCICKI. As I said in my statement, I am concerned about China and how China is leading in biotechnology, and I am concerned that China has been super clear that they would like to have the most genetic information they would like to lead. So yes, I am always concerned about what China——

Mr. GROTHMAN. Do you think a company trying to take over this company should be a company the Chinese have access to, or should they be out of the picture when it comes to a potential buyer?

Ms. WOJCICKI. I do not believe that 23andMe in this bankruptcy process should go to anyone with a Chinese tie.

Mr. GROTHMAN. Thank you.

Chairman COMER. Thank you. The Chair recognizes Ms. Randall from Washington State.

Ms. RANDALL. Thank you, Mr. Chair, and thank you to our witnesses for being here today. You know, in this modern world our sensitive data is stored in an increasing number of places. We have got smart watches that track our vitals and sleep quality and apps that track menstrual cycles and ovulation, and our phones track our steps and analyze our activity. And companies, like 23andMe, convinced so many to trade access to their DNA to unlock personal history and detailed genealogy reports. Ms. Hu, what kinds of entities are left out of our existing Federal framework for protecting health data, and how could we strengthen Federal privacy laws so that it is not left to the states to do that privacy protection work that you mentioned earlier?

Professor HU. Thank you so much, Congresswoman, and I think that this is another chance to revisit the prior Congressman's question about why it matters. I think that, you know, these types of very sensitive data can be open to exploitation, both in national security but on also consumer, you know, exploitation purposes as well. And in the absence of these comprehensive Federal laws, we

do see the need to have the states try to enact these laws that are operating to fill the gap that is left by HIPAA. So, I think in the future, we do need to look to Congress to try to create comprehensive laws that protect against the type of data sharing, third-party use, misuses, and abuses in our wearables, in our health apps, in the way in which health data is captured through telehealth systems that might not come under the protection of Federal law, and I hope that we are able to move forward with that.

Ms. RANDALL. Thank you, and you know, just level setting for folks tuning in. In 2022, the Biden Administration issued important guidance to ensure that private health information that would be covered by HIPAA and other circumstances could not be disclosed to entities seeking to investigate someone for accessing reproductive healthcare, for example, but that guidance has been withdrawn under the Trump Administration in an effort to push forward an anti-reproductive health agenda, putting both doctors and patients at risk, and discouraging folks from seeking care. I think we have to remember that, you know, these issues are intertwined, you know, who is able to access the private health data that companies now have access to under our increasingly online and, I do not know, digitized lifestyle.

You know, Ms. Hu, should Americans be concerned? What is the implication of individuals having their healthcare data being accessed? Should they be concerned that they might be investigated or potentially prosecuted in this political environment?

Professor HU. Yes, thank you so much for that question. I think that part of the concern is the way in which law enforcement or others can access this for investigatory purposes, basically doing a workaround around the Fourth Amendment protections, if it can be purchased, if it can be repackaged, sold, borrowed. You know, I think that this is the kind of data that can then end up in a way that is used against an individual without the types of constitutional protections and criminal procedure rights that they have become accustomed to.

Ms. RANDALL. Thank you. You know, we have made some progress on this in Washington State when I was there in the legislature, and I know that many other states are trying to enact these sort of shield laws to better protect the individual data of consumers, particularly their individual health and genetic data. Are there specific steps that you would recommend Congress taking to ensure that our health information, including medical records, remains secure?

Professor HU. Yes, I think that this is where we need to look at this comprehensively, not just in a siloed way, not just health data, for example, or education data or financial data, and not just a Federal or a state level issue. I think that this truly needs to be across the board. So, you had mentioned state of Washington having biometric protections, for example, as well. Not all states have that type of biometric data protections or genetic data protections, and right now in Federal law, we only have it under, for example, GINA for in the employment context, but it really does need to have that very full comprehensive approach.

Ms. RANDALL. Thank you so much. I yield back, Mr. Chair.

Chairman COMER. The gentlelady yields back. The Chair recognizes Mr. Perry from Pennsylvania.

Mr. PERRY. Thank you, Mr. Chairman. Ms. Wojcicki, when a customer comes to 23andMe, are there—I assume there is, I do not know, so I am asking—there are disclaimers? There is information where you let them know that their data is going to be obviously used to provide the information that they are looking for, their ancestry, maybe their health information, whatever you provide, right? Is there information also letting them know that it might be used, anonymously or otherwise, for other purposes when they access your service?

Ms. WOJCICKI. Great question. I appreciate that. The goal of the company has always been about transparency and choice for our customers, and it is an area I feel incredibly passionate about, that too often in healthcare, customers are not actually given transparency and choice with their information. So, when you sign up for 23andMe, it is not a simple process. There are a number of very easy-to-understand explicit consents and there is never a default. So, for example, if you go through 23andMe, we do not default you into research. You have to actively click "yes." So, during that process, it is, you know, easily a 10-minute sign up process.

Mr. PERRY. So, customers are choosing to allow, and I am just paraphrasing it the way I would say it, choosing to allow you to use their data as you kind of see fit, with who you see fit, whether it is with a pharmaceutical company, or maybe in this case—I am not saying you do—but another country. Is that generally correct? I mean, they are choosing what they allow, right?

Ms. WOJCICKI. Correct.

Mr. PERRY. Okay.

Ms. WOJCICKI. So, it is a consent form that has gone through an ethics review. It is under an institutional review board, so it specifically allows us to do research and only with qualified researchers.

Mr. PERRY. So, would you say—and this is moving into a little bit of a different direction. I will probably get back to that, but the data you said it was discarded. You used the term "discarded." Does that mean destroyed or just discarded?

Ms. WOJCICKI. Destroyed.

Mr. PERRY. Destroyed. How is it destroyed?

Ms. WOJCICKI. I am not aware of the specifics around how it is destroyed.

Mr. PERRY. It could be just thrown away. Look, I am just asking that question because you can learn a lot by going through somebody's trash, right? And I am not saying somebody did, but so in this context, as I read about you, bankruptcy does not necessarily mean the end of 23andMe. As a matter of fact, it seems like it means like it is going to continue under some other structure. Is that about right? It is not going away. It is just going to continue. Whether you buy it or whether Regeneron, 23andMe is not going, and the data is going to be around, it sounds like. Am I correct about that, or is that the goal?

Ms. WOJCICKI. That is the correct hopeful outcome, yes.

Mr. PERRY. So, is 23andMe precluded by law from selling all or some of the data or partnering with somebody that could do that,

are they precluded by law, and I am asking the question because I do not know. Are they precluded? Is your company, or the one that you started and want to have again, is it precluded by any law from using that data or partnering with somebody that could use the data any way they want, or is there any law that stops you from doing that?

Ms. WOJCICKI. I think that is a great question. I am not an expert in all the different laws. I would like to highlight there was another genetics company that just went through Chapter 11 that was successfully just sold.

Mr. PERRY. Okay. Maybe you do not know of a law that precludes. Should there be? Like, should there be? And look, consumers and American citizens or whatever have the freedom to make choices, and if you make bad choices, like, I am not using your service, ma'am. I do not want you to know. Like, I marvel at the amount of people that are concerned about the Federal government's intrusion into their personal lives but are happy to give private companies all that data, but that is their choice, and I wonder if it should be. Well, I think it should be, but what obligations do you have?

So, maybe the question should be what moral or ethical obligation does a company like yours, or yours in particular, or 23andMe may be the better way to put it, what obligation do you have to safeguard that information from either being purchased or through partnering with somebody, like the Communist Party of China or somebody affiliated with them or the People's Liberation Army? What moral and ethical obligations do you have?

Ms. WOJCICKI. I think the most important thing that 23andMe can do is make sure that we are always giving people choice, and I think that the most important thing in this process is to make sure long-term that customers always have that opportunity to delete the data.

Mr. PERRY. Yes, I understand that, ma'am, but you are not answering my question. What obligation does your company or companies like yours have, knowing that this is personal information, that it could lead to national security implications and certainly personal implications that are deleterious to those who subscribe, what obligations do you have or should you have or a company like yours have? What obligations, moral or ethical?

Ms. WOJCICKI. So, I think there should be. I think that is why we are in a bankruptcy hearing where there is oversight on it and very concerned about where it is going, and that is specifically why I have put in a bid as a nonprofit entity to acquire it.

Mr. PERRY. I yield.

Chairman COMER. The gentleman yields back. The Chair recognizes Mr. Subramanyam from Virginia.

Mr. SUBRAMANYAM. Thank you, Mr. Chair. As mentioned before, I think it was 15 million people have now signed up and used the service over the years. It is a large number, and I was one of them. I actually got it for free. I was lucky enough to get a free kit, and at the time I said, you know, what is there to lose, but I guess now, as my dad says, everything has a price, right? Nothing is free in life. And so, I think a lot of people are concerned about the fact that they did this many years ago, they are worried about what is

going on with their data, and they feel like they do not have a sense of control anymore. And you know, what I am hearing is that they do have control, though, right, in the sense that they can go online and delete their data. But when I go to the website on *23andme.com*, it is not readily apparent that 23andMe is going through a bankruptcy right now. In fact, it is not anywhere on the front page of the website. You really have to dig into the website to look into it. I have it up right now.

And the other part is there are instructions online on how to delete your data, but even that stuff is kind of buried a little bit. You really have to look for how to delete your data. I am actually going and doing it right now, and one of the things it does is you have to go to the settings page, but you have to scroll through the settings page and you may almost miss it. And then you click on your 23andMe data, and then even that, it goes through a whole list of things that are happening. And if there simply was a delete my data page or button somewhere more prominent, then I think it would be easier for a lot of people to feel that control, and this process would be a lot easier for people who do truly want to delete their data, but that is not quite what is happening.

The second thing is, you know, if I did not know about this, I was not reading the news about what is going on, I would also not know until maybe it is too late what has happened to my data and where it ended up. And so, I guess my question—maybe this was already asked—Mr. Selsavage, if you sell the data to a third party in this bankruptcy, can they sell the data to other companies after that?

Mr. SELSAVAGE. So first, let me address a couple questions.

Mr. SUBRAMANYAM. Well, just answer my question. Can they sell the data? Can the company that receives this data through a sale and bankruptcy then sell the data to another company?

Mr. SELSAVAGE. Two potential companies that are acquiring 23andMe as potential bidders are adopting and stepping into the shoes of the company and adopting the privacy policies and consents.

Mr. SUBRAMANYAM. But they could sell it to a company that then sells it to another third party, who then sells it to another third party, and then you end up with a situation where the genetic data is out there and multiple companies own my genetic data and the millions of people's genetic data. Is that correct?

Mr. SELSAVAGE. Congressman, with all due respect, I am not a legal expert in this, but basically, the potential acquirers of 23andMe are adopting the privacy policies and consents of 23andMe where it does allow for the sale of the assets of the company.

Mr. SUBRAMANYAM. So, yes, the answer to my question is yes. So, then, if, let us say a healthcare company bought the data, Professor Hu, couldn't the healthcare company then look at your genetic data and raise your premiums because they see some bad genetics in there, for instance? Can we have a healthcare system that now has all your genetic information and then will adjust premiums based on what they think is risk for them?

Professor HU. Yes, thank you so much, Congressman, for that question. I do think that genetic data is particularly sensitive because of those types of risks, that the way in which you do have

insurance companies and other corporations trying to link up genetic predispositions, even, for example, you know, financial literacy and accountability, so not just for insurance issues. Perhaps even other types of issues could be open to abuse.

Mr. SUBRAMANYAM. And then couldn't a foreign actor either hack into the data or even acquired the data as well and then use that and posing a national security threat?

Professor HU. Yes, absolutely. I think that part of what was deeply concerning, I understand about the issue of credential stuffing as the source of the cyberattack or the risk, this and the prior breach, but nonetheless, what we did see was a hacker named Golem post the DNA, particularly of the Chinese and Jewish ancestry on the dark web.

Mr. SUBRAMANYAM. I just deleted my data. I hope everyone at home has the opportunity to do so, does so, and I hope a good actor does buy this data because it could slip into the wrong hands. I yield back.

Chairman COMER. Very good. The Chair now recognizes Mrs. Luna from Florida.

Mrs. LUNA. Hey, everyone. Thank you so much for coming in today. Specifically, thank you for your work on the human genome. Aside from that, this is pretty quick on questioning. My question for you guys is, we talk about if people want to actually delete their data, just so I am clear and so people watching this are clear, in the event that they choose to opt out, delete their data, what happened to the data? Is it gone forever? Is there, you know, an area where it can be pulled back up after deleted? What happens? Ms. W, if you will.

Ms. WOJCICKI. I appreciate that. During my tenure when I was CEO, and I can only speak about that since I have not been there since March, if a customer wanted to delete their data, it was irreversible. It was gone, so if you wanted to delete your data, it was gone.

Mrs. LUNA. Okay. So, there is no way that they can bring it back up after the fact?

Ms. WOJCICKI. No, it becomes an issue then. If people want to upload it again, you would have to re-spit.

Mrs. LUNA. Okay. Perfect. Well, thank you. That is all for my line of questioning. Does anyone else want my time? No. That is it. Thank you guys.

Chairman COMER. The Chair recognizes Ms. Lee.

Ms. LEE. Thank you, Mr. Chair. I think what we have seen in both last week's hearing on AI and today's is how unprepared this country is to protect people's private information. This bankruptcy and the sale of 23andMe demonstrates just how little control people actually have over their sensitive information. The few Federal privacy laws we do have on the books have just not kept up with the internet age and the technological advancement. As a result, more and more of our data is just accessed by more and more interests, and it is just out there. Companies are handing over private data to the government that would normally be protected by the Fourth Amendment, for instance, and you would need a warrant to get. That includes genetic data at 23andMe. Some states have, of course, pushed for stronger consumer protections around privacy,

but the data threats are not stopped by state lines, so people need protections that cover the entire country.

Professor Hu, just briefly, what is your biggest concern about the gaps in privacy law that Congress ought to address through legislation?

Professor HU. My deep concern is the way in which AI is changing, I think, the nature of data. I think that, as it has been explained before, data is to AI the way that airspace is to aircraft, and without being able to have a way in which to really protect it and secure it, I think that we are going to increasingly see abuses, misuses, and discrimination flow from that lack of regulation.

Ms. LEE. Thank you. The patchwork of privacy protections in this country has created an ecosystem where data brokers and companies like 23andMe hold massive amounts of sensitive information from millions of Americans and they can just really do what they want with it. Beyond just collection and storage of data, we should also be worried about how these companies use this data, including who has access to it, for one, law enforcement officers. There are few restrictions on law enforcement's access to DNA profiles stored in databases, like 23andMe. This so-called forensic genealogy is often done without a court-approved warrant and can mean that law enforcement has access to the genetic information of millions of Americans with little to no oversight. Even if you, yourself, did not give your DNA away, if you have a family member who did, you could be affected.

What is even worse is that people usually are not even aware that their profiles are being shared with police. 23andMe's current privacy policy states that when faced with law enforcement requests, the company will "only comply with court orders, subpoenas, search warrants, or other requests that we determine are legally valid." Mr. Selsavage, that last part is a bit concerning. What exactly do you mean by other requests that are legally valid, and what other request is going to get 23andMe to give over information to police?

Mr. SELSAVAGE. Let me first say that 23andMe, to date, has not given any information over to law enforcement. We have a transparency page on our website, which shows the requests that we have received from law enforcement. It is a small number and those that we have complied with, and you will see that it is zero that we have complied with. The only way we will comply with a law enforcement request is with a legally valid process, such as a court order or subpoena, and to date——

Ms. LEE. Yes, I see that. Just really specifically, just really wondering about the other requests that we determine, I get the subpoenas and a search warrant, but there is a caveat for other requests that we determine are legally valid. Can you give an example of what that might be?

Mr. SELSAVAGE. I cannot give an exact example of that "other", you know. I can say that, you know, basically the only way we would comply with a law enforcement request was with what we determined——

Ms. LEE. Thank you.

Mr. SELSAVAGE [continuing]. To be a legally valid process.

Ms. LEE. Thank you. I think of the fact that you cannot define what that means is a massive loophole for 23andMe to do what it wants with people's data, and that is, I think, a really big concern. Mr. Selsavage, also, how does 23andMe notify a customer when it has provided their genetic data to law enforcement? I am sorry if you already answered that. What information do you provide them about the requests?

Mr. SELSAVAGE. As I mentioned, to date, we have not provided any information to law enforcement.

Ms. LEE. Yes. If you did, do you have an example? Do you know what the policy would be about how you would notify them?

Mr. SELSAVAGE. I do not, but I can take that back to our team.

Ms. LEE. Thank you. I appreciate that.

I think these policies have a lot of room for improvement and that your customers deserve better, but it is at least a baseline, hopefully, of protection. Can you commit that 23andMe will not get rid of this policy regardless of who ends up owning it once the bankruptcy sale goes through?

Mr. SELSAVAGE. I can say that the two bidders for the company have both agreed, both, you know, verbally and in writing in their contracts to purchase the company, that they will step into the shoes of the company and adopt the privacy policies and other consents on a go-forward basis.

Ms. LEE. God willing, I guess. It is really scary that people have to rely on the whims of a private company to protect their private information. The Fourth Amendment can only protect us so much as these loopholes and workarounds need to be fixed. So, I thank you all so much for your testimony today, and I yield back.

Chairman COMER. The Chair now recognizes Mr. Burchett from Tennessee.

Mr. BURCHETT. Thank you, Mr. Chairman. I believe you are from Kentucky, neighboring state. Ms. Wojcicki, did I get that right? Close?

Ms. WOJCICKI. Very close.

Mr. BURCHETT. All right. Well, nobody gets "Burchett' right, so do not feel like the lone ranger up here. Are you aware that in 2015, 23andMe received funds from a variety of investors, including WuXi Healthcare Ventures?

Ms. WOJCICKI. I am aware of that.

Mr. BURCHETT. Okay. And according to 23andMe, this partnership has dissolved. Is that correct?

Ms. WOJCICKI. That is correct.

Mr. BURCHETT. Do you know how much WuXi Healthcare Ventures invested in your company in 2015?

Ms. WOJCICKI. They invested $10 million out of a $115 million round.

Mr. BURCHETT. Okay. Are you aware that at that time WuXi Healthcare Ventures had direct ties to the CCP and the Chinese People's Liberation Army?

Ms. WOJCICKI. We were not aware.

Mr. BURCHETT. Can you explain how the partnership between WuXi Healthcare Ventures and 23andMe was dissolved?

Ms. WOJCICKI. I believe that they sold their shares. It was just an investment.

Mr. BURCHETT. Well, investors, though, in a corporation do have votes on things that occur, though.

Ms. WOJCICKI. They had no control.

Mr. BURCHETT. They just gave you all $10 million with no strings attached?

Ms. WOJCICKI. There was no control.

Mr. BURCHETT. They just gave you all $10 million with no strings attached? That is a yes or no?

Ms. WOJCICKI. They were just an investor. No strings.

Mr. BURCHETT. Okay. I have a bill, H.R. 2286. It is the American Genetic Privacy Act of 2025, and it was actually put forth last year and you all's lobbyists do an excellent job. And this Congress, as Congresses in the past, have very little guts to do what I feel like is the right thing because it takes a great deal of trust for Americans to share their sensitive genetic information with DNA testing companies. And selling this information to companies with direct links to malicious foreign actors, I feel like, is a huge violation of trust. DNA testing companies must keep Americans' genetic information private so it is not used against us by the Chinese Communist Party or any other nefarious characters.

The bill that I put forth would prohibit commercial DNA testing services from disclosing this genetic information of the United States nationals to the CCP or entities affiliated with it. And if we had passed this, and it does not come through this Committee, it is another committee, but if we had passed that, we would be probably, the questions would be a little different up here. I was made aware of a situation where supposedly the Chinese could say they collected this data that was sold to them on the market, and they would do a genome, which I understand is a study of genetic information, and develop a pattern. And they could possibly develop diseases or something, a bug along that line, that could say, stop American women at childbearing ages from bearing children. And this was discussed up here, yet we have not brought forth any legislation to stop that, and that was over a year ago under a previous administration.

To me, that just shows the gutless nature of Congress and of us, and our greed and the power of the power of the K Street lobbyists. I would hope that this body and the media would bring attention to this problem. To me, it is a serious breach of ethics but our national security, and it should go past parties and pointing fingers. We just need to get some legislation filed, and we need to enforce it. It is worthless when we pass these worthless bills, these so-called studies. And then what happens is we get a good piece of legislation, you have got a committee that goes forth with the legislation, you have a well-intended Congress person, yet a staff person, the lobbyists have their ear and they stop that legislation for whatever reason. They say, we want you to do something, but we need to do a study.

Well, folks, if you have ever seen the movie "Raiders of the Lost Ark," where at the end, there is a warehouse full of this stuff, of things that we are supposed to be looking at, that is what I believe these studies go to, is there is some worthless warehouse, and we go home and we tell everybody, look what we did, and we do not do a dadgum thing up here. We have got to get past the greed and

the gutless nature of this thing. We need to take our dadgum country back, and both parties ought to be ashamed. Mr. Chairman, I yield back the remainder of my time.

Chairman COMER. The gentleman yields back. The Chair recognizes Ms. Tlaib from Michigan.

Ms. TLAIB. Thank you, Chairman Comer. You know, Americans are rightfully worried. I know the professor knows and probably hears from a lot of folks about corporations and how our government is allowing them, like 23andMe and others, to use and sell deeply personal information, including medical and genetic data. I want to tell my colleagues, and I am glad to hear some of them speak up about this because sometimes I feel like our country has gradually turned into a surveillance state where everything about who we are, what we do is generating private profit and leave us without any privacy: surveillance pricing in grocery stores, come on; the NSA spying on our private communications; insurance companies using discriminatory factors based on our private medical and genetic history. I do not know any American, Republican, Democrat, Libertarian, independent, whatever the labels that they put out, wants to live like that. No one does.

So, Professor Hu, you know, how can we ensure that genetic data of 15 million users as 23andMe is being put for sale, will not be used for private actors? And I just wanted to be clear: I know everybody is talking about China, but I am actually really worried about corporate greed here in our country. You know, to me, corporate greed in our country is a disease. It is causing more death. I do not care if it is a fossil fuel industry, what my residents call sick care, not health care in our country, whatever it is. But I am really worried, Professor Hu, because, Professor Hu, I can see healthcare insurance companies using data saying, your genetics shows you might get breast cancer, we are not going to cover you, you are not going to get life insurance, you are not going to be able to get access, or they are going to, again, use this to profit, not to help. We do not seem to prevent death and destruction in our country. Even this chamber does not do that, and so what can we do? I mean, this is genetical, medical, you know, history. As you know, it is incredibly important, especially, you know, I know a lot of ethnic and racial heritage is also mixed up in there, and you saw them targeting folks of Jewish faith, and again, is just to me watching this happen, and then we do nothing. We will have this hearing, and I know Chairman Comer is trying to do his best, but we are going to have this hearing, but are we going to actually update HIPAA? Are we going to actually do something to push back against, you know, profit for this kind of data and information?

Professor HU. Thank you so much, Congresswoman, for that question. And I do think that this is a moment to assess first principles in our commitment to the Constitution and to what extent does the increasing privatization and commodification of this data come into conflict with our core values, but not only just our constitutional values, our national security interests, and the way in which our national security interests are infused by these fundamental commitments to rights and liberty and freedom and expressive rights and privacy rights as anchoring how we see, you know, ourselves as a Nation.

So, you know, your question about, you know, what can we do to stop drifting into a surveillance state, I do think that one of the things that we need to make sure that we understand is that our ability, I believe, for us, to remain dominant geopolitically is not about deregulation or de-devolution of the regulations around data privacy, cybersecurity, and AI but leaning into them so that we can make sure that these systems unfold safely and securely, and other nations are now embracing these types of legal regimes, including China, and we are not. And I think that that puts us at a great national security disadvantage.

Ms. TLAIB. I agree. I think for many of our colleagues here, you know, expressing on X your concern and everything about like, again, privacy is important, but I think we need really comprehensive data that protects the Americans' private data. I mean, this is literally going to be a fight between the corporate greed and the government surveillance and how overreaching that is because it is, again, going to be profit before the people, and many of them are going to 23andMe because they want to live. They want to live. They do not want to get sick. They want preventive care.

And I know, like, you know, the Trump Administration right now is destroying privacy protections. I see it raiding private Social Security data, tax info, bank account numbers, you name it. I am really concerned about this growing factor, but I also want many of my colleagues to know, I mean, Trump is now working with data and surveillance companies like, what is it? Palantir—is that how you say it—I mean, look at this, to compile databases on Americans. First to target immigrants. They always start there, and then they are going to target, you know, it is going to be other folks. It is going to be unbelievable because, you know, Peter Thiel and Alex Karp, who made it clear that they care more about political domination than American democracy or individual privacy.

I say this because we are talking about 23andMe, but understand there is a bigger movement in our country that we need to put in check right now because they do not care about us. They do not care about the folks that put us here and told us to protect them, and so I think it is really important, Chairman, after this hearing, let us not just have it in the congressional Record. Let us actually do legislation to hold them accountable. With that I yield.

Chairman COMER. The gentlelady yields. The Chair recognizes Mr. Burlison from Missouri.

Mr. BURLISON. Thank you, Mr. Chairman. Professor Hu, it has been talked about a lot in this hearing about the potential threats and risks of, you know, a foreign actor getting access to, you know, Americans' DNA records. Can you elaborate on what is the potential risks that we are facing?

Professor HU. Yes. Some of the risks include, for example, blackmail, using it in order to exploit and try to make individuals more vulnerable, greater surveillance risks, and as was discussed, potential biochemical, biometric types of warfare. But I do think that there are also potential AI-driven targeting risks as well.

Mr. BURLISON. And then, you know, this is not new. I mean, the hospitals, providers, their electronic medical records, they are tempted to be hacked all the time. Have you heard of what the street value of someone's medical record is? At one point I had

heard that it is over $50,000 or more. It is probably a lot more today. Mr. Selsavage, one of my questions has to do with how the hack occurred in 2023. Is it correct that individuals who had stolen, you know, passwords from other businesses then use that in a form that is called stuffing, where they used an automated system to take, say, the hacked passwords and accounts from another company and then just rolled through those to see if those same passwords were used on your site. Am I getting that accurately?

Mr. SELSAVAGE. That is generally accurate. It is something called credential stuffing, whereby a user, you know, and we all have done this, has used the same username and password on multiple websites.

Mr. BURLISON. Right.

Mr. SELSAVAGE. And other websites were hacked, and they were able to obtain those usernames and passwords, and then they tried them on 23andMe and they were able to access a number of accounts, to get into and take the DNA relative information.

Mr. BURLISON. And so, the mechanisms that you have put in place to stop that from happening in the future are that you send a text message to verify that somebody is logging in from, that was the original individual. What other steps do you take?

Mr. SELSAVAGE. You know, right after the cybersecurity incident, the first thing we did was force every consumer to reset their password, and as part of that process——

Mr. BURLISON. They could not use the previous one.

Mr. SELSAVAGE. They could not use the previous one, and we also checked that password against known hacked passwords, right, just to make sure that, you know, the same thing wasn't going to be happening with another credential stuffing.

Mr. BURLISON. I think if the American people are listening, you should never use the same password for different website businesses.

Mr. SELSAVAGE. That is a very good process.

Mr. BURLISON. Just a good policy to follow.

Mr. SELSAVAGE. And then second, you also mentioned we did also implement two-factor authentication, whereby, you know, basically we actually then either sent the customer a text message or an email confirming that it was them, and they entered that code to make sure that there was an additional layer of security, a second factor, to access their account.

Mr. BURLISON. Yes. Thank you. Ms. Wojcicki. Is that correct? You know, I think that one of the things that is kind of striking me is that when someone enters into an agreement, they know your company, they know your reputation, they know you. I think what we are kind of going through is a situation where potentially that what the trust that was placed in you because of this situation is in jeopardy if somebody else gets access to that information. The question is, what will they do with that? So, one of my questions is, do you think that there should be a law that upon the sale of a business that an individual has to reconfirm that they want the new company to have access to their data?

Ms. WOJCICKI. Thank you for that question. I am a huge believer that people should have choice in transparency. So, I think it is a complicated question, the one you just asked, because there are in-

dividuals, for instance, like my sister, who recently passed away of lung cancer, who established a lung cancer community in 23andMe, and feels very passionately about identifying genetic risk for non-smoking lung cancer. So, she is deceased. She opted in to research because she really cared about that mission, and it was really important for her. You know, lung cancer is massively underfunded, it is one of the poorest-funded areas, so how could we all come together? So, how could she possibly reconsent?

Mr. BURLISON. I just have one more question. So, when a separate company that you have created, have a contract with you and you shared some of that data, what mechanisms do you have to protect and make sure that company is not then reselling it and sharing that data?

Ms. WOJCICKI. That would have been part of the contract. So, for example, with GSK, they were looking at aggregate statistics, they could not go and then share that with other partners.

Mr. BURLISON. Okay. Thank you. I yield back.

Chairman COMER. The Chair now recognizes Ms. Pressley from Massachusetts.

Ms. PRESSLEY. Ms. Wojcicki, you claimed that 23andMe is all about consumer empowerment, but most people ended up actually exploited, not knowing that they signed up to have their genetic data auctioned off to the highest bidder. We are not just talking about email addresses, we are talking about names, birth dates, genetic lineages, literal DNA, data that implicates entire families, not just the person who gave the sample. Ms. Wojcicki, can genetic data, even if de-identified, be linked back to individuals?

Ms. WOJCICKI. I appreciate that question. Could genetic data be linked back to individuals? You can link back. Your DNA is your DNA. If I have a way of matching it to something that potentially connects to you, then you could potentially identify.

Ms. PRESSLEY. So, the answer is yes. The answer is yes. The genetic data, even if de-identified, can be linked back to individuals, just the science?

Ms. WOJCICKI. No. DNA, if I had your sample, essentially, if I know what your picture looks like and I see another picture, I can connect those, but just having your DNA alone, if I just went to the subway and I swabbed it and I looked at samples, I would not be able to identify who is there.

Ms. PRESSLEY. Let me reclaim my time because I do not have much of it and there is a lot of ground I need to cover here, and so I want a more direct question here. So, I am going to go to Ms. Hu. Is de-identified genetic data truly anonymous or can it be traced back to individuals? Ms. Hu.

Professor HU. Thank you so much, Congresswoman. I am not a scientific expert on that exactly, but there has been research on the limits of de-identification and also the risks of re-identification.

Ms. PRESSLEY. All right. Fair enough. Yes, it absolutely can. With just a few pieces of additional information, like zip codes, gender, or 23andMe's Find Your Relative feature, it becomes easy to re-identify people and to expose their personal health information. 23andMe's privacy agreement talks about anonymous data, but DNA can never truly be anonymous. That is the point.

Now, Ms. Wojcicki, you said a limited number of customers were compromised by the data breach, but the truth of the matter is that out of the 15 million people who trusted this company, half of them, seven million, had their data exposed. So, that is not inconsequential. It is deeply consequential. And now, that same data can be sold off to a for-profit pharmaceutical company, so you can understand why people are rushing to delete their accounts. But the thing is, when people have tried to log in and delete their data, they received error messages, and then the website crashed. That is not okay. Your company is preventing people from deleting their information.

Mr. Selsavage, it is time to put people first. Will you contact each of your customers seeking consent for 23andMe to continue holding their data? Yes or no, your simple opt-in communication that you send out before any bankruptcy sale. I want to really underscore that.

Mr. SELSAVAGE. Congresswoman, we first have sent a notice out to all of our customers via email——

Ms. PRESSLEY. Reclaiming my time, Mr. Selsavage.

Mr. SELSAVAGE [continuing]. Notifying them of the sale. A second email is currently going out this week, notifying them that the sale——

Ms. PRESSLEY. Mr. Selsavage, reclaiming my time. Please just answer the question yes or no, okay? Will you commit to contacting each of your customers seeking consent for 23andMe to continue holding their data? This should be a simple opt-in communication that you send out before any bankruptcy sale. Yes or no.

Mr. SELSAVAGE. Congresswoman, it is not that simple. We believe we have already received consent from them.

Ms. PRESSLEY. Why not? These people are deserving of these assurances and this insurance. They have been violated in so many ways here. Ms. Wojcicki, will you amend your bid to commit to a similar consent requirement then?

Ms. WOJCICKI. I do not believe I can talk extensively about my bankruptcy, about the bid, but I can say in the past, for example, when we did the GSK partnership, we proactively communicated with all customers.

Ms. PRESSLEY. I know that, I know that, I know that, I know that. It is not good enough. It is not good enough. It is just not good enough. People trusted you with their more personal information. Show them you respect them. They do not need your apologies anymore, and they do not need your sympathy. What they need is legal protection. So, if you are not able to protect the 15 million people and their families who trusted you, this company should not exist. The breach of data, the breach of civil liberties, the confusion this has caused for millions, it might just be time to give it up. I yield back.

Chairman COMER. The Chair now recognizes Mr. McGuire from Virginia.

Mr. MCGUIRE. Thank you, Mr. Chairman. Thank you to our witnesses for being here today to answer our questions regarding the safety of millions of Americans' genetic information and personal data. If malign foreign actors such as the Chinese Communist Party, CCP, were to get their hands on the data, the privacy of mil-

lions of Americans and our national security will be at risk. And I apologize if I do not pronounce your name right, but Ms. Wojcicki. Is that right?

Ms. WOJCICKI. That is great.

Mr. MCGUIRE. We know approximately 15 million customers have submitted their DNA samples for genetic testing to 23andMe. Do you know roughly how many of these customers are American citizens?

Ms. WOJCICKI. I believe the last when I was there, it was about 85 percent of customers were from the U.S.

Mr. MCGUIRE. Thank you, and, Ms. Wojcicki, yes or no. Did 23andMe already give Chinese corporations associated with CCP and the Chinese People's Liberation Army access to this data?

Ms. WOJCICKI. To the best of my knowledge, since I have not been there since March, no.

Mr. MCGUIRE. Understanding that every company in China is associated with the CCP. All right, Ms. Wojcicki, 23andMe received investments from WuXi Healthcare Ventures, a company tied to the Chinese People's Liberation Army and CCP. What other foreign entities have invested in 23andMe?

Ms. WOJCICKI. In 2018, 23andMe had an investment from GlaxoSmithKline, which is a U.K.-based operation.

Mr. MCGUIRE. And Mr. Selsavage and Ms. Wojcicki, yes or no. Would you be comfortable with your or your family's genetic information and sensitive data being in the hands of a malign foreign actor such as CCP? Yes or no.

Ms. WOJCICKI. I would not be comfortable.

Mr. SELSAVAGE. I would not be comfortable.

Mr. MCGUIRE. All right. follow-up: what steps are you taking to ensure the sensitive data of millions of Americans is secure and will not be sold to malign foreign actors?

Mr. SELSAVAGE. I can take that question.

Mr. MCGUIRE. Thank you.

Mr. SELSAVAGE. You know, as part of the bankruptcy 363 sale process, we have, you know, special committee has affirmatively said that the company will not be sold to any entity in China, Russia, North Korea, Iran, or any other foreign adversary. I am happy to report that through the bankruptcy process, we, at the current time have two final bidders, both American enterprises: TTAM Research Institute, which is an American foundation, and second is Regeneron Pharmaceuticals, which is an American pharmaceutical company, here as a public company.

Mr. MCGUIRE. There will be dire consequences to our national security as well as the privacy of millions of Americans if the CCP or other malign foreign actors are able to gain access to sensitive data of 23andMe. The CCP and any of the foreign actors should not be allowed to gain access to millions of Americans' sensitive data, which can then be weaponized against them through surveillance or even the creation of a bioweapon. It is our duty as Members of Congress to protect our constituents' privacy and our country from foreign actors who will weaponize this data against us if given the opportunity. And with that, Mr. Chairman, I yield back.

Chairman COMER. Would you yield a minute to me of your remaining time?

Mr. MCGUIRE. Absolutely.

Chairman COMER. How confident are you all that your data will not end up in the hands of a bad actor? Are you very confident, somewhat confident, or you have no idea?

Mr. SELSAVAGE. As interim CEO, I am very confident that, you know, the sale of the company will not result in the company being sold or the data ending up in the hands of a bad actor, and by that I am referring to China, Russia, Iran, Venezuela, or other foreign adversaries.

Chairman COMER. What about health insurance companies or things like that, American health insurance companies?

Mr. SELSAVAGE. I think I am very happy to report that the final two bidders for the company are TTAM Research Institute, which is a foundation here in the U.S., founded by Ms. Wojcicki; and second is Regeneron Pharmaceuticals. Neither of those are healthcare companies.

Chairman COMER. Yes. Okay.

Mr. SELSAVAGE. And I feel confident that they are taking over the privacy and policies and consensus of 23andMe.

Chairman COMER. Ma'am, how confident are you?

Ms. WOJCICKI. I am not involved in the bankruptcy process other than being a bidder, and so for myself——

Chairman COMER. If you end up with it, you are confident that your company will?

Ms. WOJCICKI. I am confident.

Chairman COMER. All right. The Chair recognizes Mr. Min from California.

Mr. MIN. Thank you very much, Chair Comer. I have to confess, I do not use 23andMe. I have never been tested for genetics, but I certainly have a lot of customers who have chosen to use 23andMe, and I have heard from a lot of them. But Mr. Selsavage, I understand that customers of 23andMe can choose to consent to have their individual genetic information shared with your researchers. What protections were put in place to protect your customers from the misuse of that data?

Mr. SELSAVAGE. First, you know, our customer data and our policies are always putting our customers first.

Mr. MIN. Right. Reclaiming my time. Just briefly, what protections are in place to protect your customers from misuse of that data?

Mr. SELSAVAGE. First, they can have the right to actually remove their consent to that data for being used for research policies at any time. The company always has provided researchers with deanonymized data. We are not providing individual identifiers when we actually share that data for any research.

Mr. MIN. And I believe you also have protections that it is explicitly limited to just research purposes, right? You could not, like, go ahead and sell that to Goldman Sachs, right?

Mr. SELSAVAGE. You know, first, there is a research consent that only 23 can use their data for research purposes, and there is a separate individual consent for using that data with third parties.

Mr. MIN. Right. I understand that, but I am looking at your terms of service right now, and I do not see any specific language

giving 23andMe any ownership rights to people's individual level genetic health information. Is that correct?

Mr. SELSAVAGE. That is correct. Our customer data——

Mr. MIN. Okay. Reclaiming my time. Under the section it is described as licensing and IP rights, your terms of agreement state that you get a license to use "user content," which is described as information, data, things like that, that are generated by users of the service and transmitted to you. It goes on to say specifically, "User content does not include genetic or health information." I take it from this and the fact that licensing rights for individual genetic or health data are not mentioned anywhere else in your terms of service, that you also do not receive a licensing right or royalty rights to people's individual genetic or health data. Is that correct?

Mr. SELSAVAGE. I am not a lawyer, but, you know——

Mr. MIN. You do not own it. You do not own the data individually of people. You can use it for some purposes, for research, if they consent to it, but you do not have an ownership right, isn't that? I think you just said that. Is that correct?

Mr. SELSAVAGE. That is correct. Our customers own their data, and they control that data at all times.

Mr. MIN. So, I want to re-ask the question. Could you share somebody's individual data, genetic data, with Goldman Sachs or Elon Musk or with the Chinese Government? Could you sell it to the highest bidder?

Mr. SELSAVAGE. You know, our policies state that, you know, basically we can actually——

Mr. MIN. Reclaiming my time. If I was really interested in the genetic data of Chairman Comer, could you sell? Could I buy Chairman Comer's data if he was a client at your service?

Mr. SELSAVAGE. No, you could not.

Mr. MIN. Why not?

Mr. SELSAVAGE. Because we do not have the right to share.

Mr. MIN. Because you do not own it, right? You do not own the rights to that. Could you sell the homes of your customers? Could you sell any other assets they owned? The answer is no, because you do not own that, right? So, you do not own people's genetic or health information. So, I guess I am really just wondering why you think you can sell this data at an individual level to a third-party company that is coming in. I know you are talking about protections on that data, but I am just wondering. I am not a customer of yours, but for those who are, including my constituents, why are you selling their genetic data when you do not own it?

Mr. SELSAVAGE. You know, the terms of service and the agreements at 23——

Mr. MIN. I looked at your terms of service, yes.

Mr. SELSAVAGE. It mentioned that we can basically, in the event of a sale of the company, or a bankruptcy of the company, that the data can be transferred to the new company.

Mr. MIN. Look, 23andMe, what you guys do, I think at your height, you seem like you are doing great things, but you fall into a clear regulatory gap here between HIPAA and GINA, as I think has been described. And I think this is one of those rare instances where my Republican colleagues and I all, we all agree on the prob-

lems that this raises, and I think it is clear that we need some kind of regulatory protection. So, I guess I am going to ask you, in the meantime, before we address this with law, I want to echo the point made by my colleague, Rep. Pressley, why won't you commit to what seems like a very reasonable and commonsense opt-in policy, given that you are about to sell people's individual level genetic data, very valuable information, very personal information. Why won't you commit to doing that? It seems like a very reasonable thing to do.

Mr. SELSAVAGE. Congressman, we believe our customers have already consented to the transfer of their data through the consents that they signed up for when they signed up for the service. Second, we have provided the customers with notice of the bankruptcy, and we will be providing them with notice of who the company——

Mr. MIN. Do you check every email you read?

Mr. SELSAVAGE. I do not.

Mr. MIN. I certainly do not, and we certainly might miss an email or several emails like this. And I would just encourage you to think about an opt-in policy because what you are describing right now is the transfer and sale of data that is very, very personal, and I personally find it very outrageous that you are not allowing people to opt in to this, not giving them that right, knowing that the open rates of your emails are probably very low. With that, I yield back.

Chairman COMER. The gentleman yields back. I hate to interrupt this good bipartisan hearing, but at the request of the witnesses, we are going to take a 5-minute bathroom break. When we return, Mr. Timmons will be asking questions. So, pursuant to the previous order, the Committee will stand in recess for 5 minutes.

[Recess.]

Mr. HIGGINS. [Presiding.] The House Committee on Oversight and Government Reform Full Committee hearing titled, "Securing Americans' Genetic Information: Privacy and National Security Concerns Surrounding 23andMe's Bankruptcy Sale," is back in session.

The Chair recognizes Ms. Greene of Georgia for 5 minutes for questioning.

Ms. GREENE. Thank you, Mr. Chairman. Ms. Wojcicki—I am sorry, I apologize—you co-founded 23andMe in 2006 and took the company public in 2021. Is that correct?

Ms. WOJCICKI. That is correct.

Ms. GREENE. And this is all about DNA, which we would call science. Is that right?

Ms. WOJCICKI. It was really about how individuals can learn about their genetic information.

Ms. GREENE. Right, but DNA and the study of it is science. Is that correct?

Ms. WOJCICKI. It is about learning about their family, their ancestry, science, and their health risks.

Ms. GREENE. Okay. So, it is science. Now in 2001, you reposted Dr. Raven the Science Maven, who reposted my post of a sign that I kept outside of my office that said, "There are two genders: male and female. Trust the science." And the attack on this, which you reposted, so you must have agreed with them was, "As a scientist

with a transgender parent, I need you to sit down. You do not know the science or the history. You trust the science. Science draws a difference between sex at birth and gender identity. The systematic institutionalization of gender is a product of colonization." What does colonization have to do with gender?

Ms. WOJCICKI. I have not seen that in a long time. I do not——

Ms. GREENE. You reposted it, though, so you must have known something about it. Also, 23andMe, the company that you led at the time or that you are still there and you are trying to buy, "Opponents of trans rights use the phrase 'trust the science' to make false claims about sex and gender. We support what the science actually says, accepting and affirming trans people has a positive impact on their health. Trust the science. Support trans health," which is really interesting because in DNA it shows that there are only two sexes, two genders, male and female, and that should be something that you are intimately—you know, you are very tied into that since you founded the company, co-founded the company, took it public, and you want to buy it again.

So, it is baffling that 23andMe, a company that specializes in DNA and people's very personal information and how God has designed human beings would support and continue to support the trans ideology, that this is something that can be changed. Have you ever seen any DNA or know of DNA that a biological male can give birth to a baby?

Ms. WOJCICKI. No.

Ms. GREENE. No. So, this is something that we know cannot be changed. That is scientific. That is the design of our DNA, and I do not understand, and I think most people do not understand, why 23andMe would take such a hard-left political position supporting trans rights. And here is what is the really weird part about it is. It says, "This is one of the many reasons why we have been working to improve our products for trans and non-binary customers." I thought your product is helping people understand their DNA, linking themselves with family trees, so I cannot comprehend what kind of product 23andMe could give to people who identify themselves in some other way. That does not make a lot of sense.

Another thing that is hard to understand is, you know, the beauty of DNA is that it is a beautiful design. It is God's design down to the finest detail, a granular level of how we are made, but it also helps people link with their family trees. Yet, this is a letter that you put out after the SCOTUS ruling overturning *Roe v. Wade*, and you put out a letter very much against the ruling that the right should go back to the states. And you clearly put your own personal belief in here on the 23andMe social media that you are very much for the killing of the unborn, the killing of babies, which completely would destroy what your company is all about. How can we study DNA, how can we study people's lineage if one of the very co-founders, and who wants to own the company again, supports the murder of the unborn, the murder of God's design and the murder of God's creation, which we can link it to DNA?

And Mr. Chairman, I am running out of time, but I think that is 100 percent against the science, and I think it is 100 percent against God. I yield back.

Mr. HIGGINS. The gentlelady yields back. The gentleman, Mr. Bell, is recognized for 5 minutes for questioning.

Mr. BELL. Thank you, Mr. Chair, Ranking Member, and our witnesses for being here today. And in Missouri, we are currently recovering from one of the largest natural disasters since 1959, which has left an impact statewide, with extensive damage to my district in the St. Louis region. As we recover from these storms, the threat of waste, fraud, and abuse lingers above the lives of the thousands of individuals impacted. These same individuals who are already exhausted and depleted from the mental turmoil and physical loss are now faced with the threat of fraud. Studies have suggested that individuals recovering from natural disasters are at a higher risk of being susceptible to scams. Many of these scams come in the form of imposters who are impersonating government officials, bank workers, or even FEMA employees, to acquire vulnerable information.

These fraudsters preying on these vulnerable communities use the tactic of acquiring individual's private information, like Social Security numbers, bank account numbers, and addresses, by posing as a resource to provide help but subsequently using the information obtained for their own personal gain. Ms. Hu, do you agree that access to this personal information poses a significant threat to Americans' livelihoods, especially those in vulnerable communities.

Professor HU. Thank you, Congressman. I think that you are helping to elevate one of the critical issues about data privacy, and that is the way in which it can be exploited, particularly to those who are most vulnerable. And without comprehensive privacy laws or greater cybersecurity protections at the Federal level, I fear that we are going to continue to face these types of issues.

Mr. BELL. And since we were talking about privacy, I am going to go off my remarks for a second. To the previous questions, I do not really care what your positions are on abortion. What I care about is that a woman has a right to make a decision with her own body, that people have a right to make a decision with their own body and healthcare choices. So, what we have seen with 23andMe is a breach of privacy that has left many communities vulnerable to foster attacks ranging from identity theft to risk from exposure of genetic data. I agree and recognize the need for comprehensive legislation that ensures transparency in the collection and use of personal data, along with stronger security measures and protections when it is handled by corporations, but I also know that the threat of fraud and abuse does not just lie in our corporations, but amongst our very own government.

What we have been seeing over the last couple months is one of the largest fraudsters of them all, and his name is Elon Musk, who this Committee refuses to bring to this to a hearing to question. Musk, who has scammed the American people with false promises of efficiency and elimination of waste, fraud, and abuse has carried out the exact opposite. Musk and his DOGE team, or whatever you want to call them, have ransacked multiple Federal buildings under false pretenses, gathered sensitive and personal data and vanished, leaving others to pick up the pieces and rebuild. Sounds pretty similar to the tactics of disaster frauders to me.

It is our duty not only to hold corporations accountable, but also to hold anyone accountable who violates the privacy and safety of the American people. I will continue calling out and fighting back against fraudsters and protecting the individuals who need it most. Thank you, and I yield back to the Ranking Member.

Mr. HIGGINS. Does the gentleman yield his time back?

Mr. BELL. To the Ranking Member, yes.

Mr. SUBRAMANYAM. Thank you for that. I yield back.

Mr. HIGGINS. The gentleman yields. The gentleman from Arizona, Mr. Biggs, is recognized for 5 minutes for questioning.

Mr. BIGGS. Thank you, Mr. Chairman, and thank the witnesses for being here. I want each of you to answer this question as succinctly as possible. Who owns the genetic information at 23andMe? Ms. Wojcicki?

Ms. WOJCICKI. What we have said in the past is that you, you are the individual, always owns their genetic information.

Mr. BIGGS. Okay. So, look, I am going to leave it right there. The owner, you have said, basically the person who submitted their genetic information. Mr. Selsavage?

Mr. SELSAVAGE. The owner of the genetic information is the customer at 23andMe.

Mr. BIGGS. You agree with that, Professor Hu?

Professor HU. In their terms, they say that they can sell data.

Mr. BIGGS. Okay. Yes. So, yes, not that they can sell, but that the actual ownership rights, and when you own it legally, you got a bundle of rights. And then I think, Mr. Selsavage, you said that there is a license for use, and, Ms. Wojcicki, I thought I heard you say that, too, that that somebody opts in, they are providing a license for use, either for research or other use. Is that fair? You are operating under license agreement at that point?

Mr. SELSAVAGE. Our customers basically provide consent for us to use their data.

Mr. BIGGS. Strike that. Let us hold on.

Mr. SELSAVAGE. Okay.

Mr. BIGGS. Let us not get funny with words. Are you given the license to use it?

Mr. SELSAVAGE. Congressman, with all due respect, I am not a lawyer.

Mr. BIGGS. Okay.

Mr. SELSAVAGE. You know, I do know that our customers are always given the right to consent or remove that consent to use their data for research purposes.

Mr. BIGGS. Okay. All right. So, we will leave it there for a second, and let us just get to liability because even in a license agreement, you can breach a license agreement, and even if someone provides consent, you can abuse a consensual arrangement. And the question is, who has liability at that point, and I would suggest to you, 23andMe does. Would you agree with that, Ms. Wojcicki?

Ms. WOJCICKI. I am not sure I understand the question.

Mr. BIGGS. If you guys, 23andMe, were to violate what apparently is not a license but some kind of consent agreement, you would have a liability for that, for failure to protect the markers?

Ms. WOJCICKI. If 23andMe violated the consent, yes, then I would believe there would be an issue.

Mr. BIGGS. Mr. Selsavage, you agree with that?

Mr. SELSAVAGE. Yes, I believe 23andMe has a duty to uphold the consent that our customers have agreed to and that we have agreed to with them.

Mr. BIGGS. Okay. Professor Hu?

Professor HU. Then yes, in the breach litigation, I think the class action shows that there was liability.

Mr. BIGGS. Right. And so, let us now compare to just national security for just a moment. Professor Hu, what specific vulnerabilities in our current laws allow this data to be exploited, the data we are talking about that 23andMe is sitting on?

Professor HU. Yes. I am deeply concerned that if it is, you know, faced with foreign investor, which has already been brought up, whether or not there could be other ways in which there could be, once there is a breach, that it can fall into a foreign adversary's hands.

Mr. BIGGS. Let us get back to the liability for just a second again because this is driving me crazy. As one who owns the genetic information—let us say I did—at any point you said I can withdraw consent. Can I order you to destroy that genetic information?

Mr. SELSAVAGE. Yes, you can. Our customers always have the right of ownership. They can have complete control over their data. They can access it, and they can edit it.

Mr. BIGGS. So, I am talking about, specifically, the sample as well as the data. Do you agree with that?

Mr. SELSAVAGE. Yes. They can request a deletion of their data, which we will, and we would delete that data, and at the same time, if we had a saliva sample, which they agreed to have biobanked, we would destroy that as well.

Mr. BIGGS. Professor Hu, Americans are really concerned about domestic surveillance programs. Believe me, FISA has been abused by our own government, et cetera. How can Congress prevent the U.S. Government from having unauthorized access to 23andMe's genetic data?

Professor HU. I think that what we need is to expand HIPAA, and we need to expand GINA. We need to have greater, I think, protections and cybersecurity assurances.

Mr. BIGGS. So, I am going to lay this at you. With the abuse of FISA that we have seen, and these are massive databases being accumulated on American citizens, and inquiries being made by the FBI without any kind of judicial authority, nor with consent of the individual, do you think, Ms. Wojcicki and Mr. Selsavage, that 23andMe has taken adequate protective measures to prevent incursion from any state or non-state actor? I mean, you know you had the problem where you were hacked. So, what have you done then to make sure that you are secure against even things like the U.S. Government? And as a compound question, have you ever received a request from the Federal government or any other governmental entity to have access to a particular DNA sampling that perhaps might be in your database?

Mr. HIGGINS. The gentleman's time has expired, but the witness will be allowed to answer the question.

Mr. SELSAVAGE. Okay. I will take the second question first. You know, the company has published, you know, on our transparency

page, which is a public page on our website, you know, requests that we have received from law enforcement with regard to DNA data that the company has held. At no time have we actually provided that data to law enforcement or other authorities. Second, you know, basically, after the cybersecurity incident, we have taken additional steps to secure the data that we have at 23andMe from both, you know, foreign actors or any type of threat actor, including, you know, providing additional encryption over the data, you know, hiring, putting in additional security measures. And for simple access to customer accounts, adding in two-factor authentication and requiring all our customers to reset their passwords and ensuring those passwords and usernames have not been used in other compromised websites.

Mr. HIGGINS. I thank the gentleman. Mr. Timmons from South Carolina is recognized for 5 minutes for questioning.

Mr. TIMMONS. Thank you, Mr. Chairman. I want to focus on the potential of your data being used for bioweapons. You have the second largest collection of DNA behind AncestryDNA. Is that correct?

Mr. SELSAVAGE. That is correct.

Mr. TIMMONS. So, the internet says 25 million is what AncestryDNA has. You are at, what, 14 million, 15 million?

Mr. SELSAVAGE. That is correct.

Mr. TIMMONS. And you agree that there is the potential that a rogue actor or an evil nation-state could use the genetic data that you or AncestryDNA has gathered to then create a targeted bioweapon that would target people of certain geographic locations, ethnicity. You could even do eye color. Is that scientifically possible? Would you agree? You are not a scientist, but——

Mr. SELSAVAGE. Congressman, I am not a scientist, but I understand.

Mr. TIMMONS. Well, the research abounds, really, the last two decades, it shows that should a nation-state or a well-funded rogue actor be willing to engage in such atrocities, they could do that, and realistically, in order for that to be effective, they would need a very large amount of data from all over the planet. As you consider how this bankruptcy is going to be resolved, is that front of mind, or are you going to make sure that the vast amount of data that you have is not going to fall into the hands of an evil actor. Is that fair?

Mr. SELSAVAGE. That is fair. First, let me say that as part of the bankruptcy process, the special committee of 23andMe has committed to ensuring that under no circumstances will we sell this data to any foreign adversary, including any enterprise controlled by China, Russia, Iran, Venezuela, North Korea, or any foreign adversaries to the United States. Second, you know, we have two final bidders in the auction process for 23andMe, both of those, TTAM Research Institute and Regeneron are American enterprises. Regeneron an American pharmaceutical company, a public company with $55 billion——

Mr. TIMMONS. Thank you for that. That is helpful. Before I go to Ms. Wojcicki, I want to point out that while every individual technically owns their data that you have, it is comical to think that that ownership is real, because the likelihood of even one percent of the individuals who have used your service asking you to

delete their data is virtually zero. I actually did 23andMe, so I mean, while I do own my data and I could probably log in and try to figure out how to delete it, I am not going to do that. Nobody else that has used your business is going to. Ms. Wojcicki, when you were CEO, did you or your board ever consider the national security implications of selling licensing or sharing genetic data with research institutions abroad, including those in China?

Ms. WOJCICKI. We talked about things like that extensively.

Mr. TIMMONS. And did any foreign actor attempt to purchase any data for research purposes or other?

Ms. WOJCICKI. No.

Mr. TIMMONS. So, WuXi Heathcare Ventures was an investor. They had direct ties to the CCP and the PLA. Is that—they were just, we will give you money but we want to hear about what you are doing but we do not need any from that, is that fair?

Ms. WOJCICKI. It was $150 million that we raised in that round. They were a $10 million investor. They had no board seat, no access.

Mr. TIMMONS. And your investors have no access to any information?

Ms. WOJCICKI. No access to information.

Mr. TIMMONS. But they would get, I would imagine, industry updates that show progress?

Ms. WOJCICKI. I do not have access to my records. I do not believe they were a large enough investor.

Mr. TIMMONS. Is it fair to say that AncestryDNA has continued to be successful versus 23andMe largely because they stayed focused on giving customers their ancestry history as opposed to 23andMe was, kind of, trying to engage in secondary lines of effort? Genetic testing to, kind of, help people understand potential health issues they could have? Is that where things might have gone wrong?

Ms. WOJCICKI. *Ancenstry.com* actually has a very expensive monthly subscription to be able to look at old historical records. Versus 23andMe has really been about the acceleration of knowledge around human genetics for the benefit of all of us to be healthier.

Mr. TIMMONS. So, they were successful where you all have clearly failed because they just stayed true to the main business model and you all expanded, is that fair?

Ms. WOJCICKI. I would say, our mission, since the beginning, was to help people access, understand, and benefit from the human genome. And that benefit has always been about the benefit of human health and that understanding. So, the two companies are incredibly different.

Mr. TIMMONS. Okay. Thank you, Mr. Chairman. I am out of time. I yield back.

Mr. HIGGINS. The gentleman yields back. The gentleman from Texas, Mr. Sessions is recognized. I stand corrected. Mr. Frost is recognized for 5 minutes for questioning.

Mr. FROST. Thank you, Mr. Chair. The Federal government must play a bigger role in protecting our personal data, not just from criminals or foreign adversaries, but from law-abiding American companies as well. 23andMe holds the genetic information of more

than 15 million people and is one of the largest collections of human DNA in the entire world. They have complied with our very basic laws by not sharing data with insurance companies or law enforcement unless legally required, and providing some terms of service disclosures up front, but that is not enough.

Printed here is the terms of service and U.S. privacy policies that users review before opting in. It is about 20 pages. Buried in the privacy policy are the lines, "If we are involved in a bankruptcy, your personal information may be accessed, sold, or transferred as a part of that transaction." Mr. Selsavage, did I say it right?

Mr. SELSAVAGE. That is correct.

Mr. FROST. Do you know approximately how many people read online terms of service that they agree to?

Mr. SELSAVAGE. I do not, but, you know, one thing we did——

Mr. FROST. It is about ten percent, less than ten percent. Less than ten percent of people will read the online terms of services that they agree to, according to the Pew Research Service. 23andMe customers are now panicking. Simple notice is not going to be enough. Professor Hu, why does our personal genetic information hold so much value in the open market?

Professor HU. Thank you for that question, Congressman. I think that it is highly incentivized by the black market because of the way in which it can be exploited and the way that it can be used, especially in our AI age. I think that, increasingly, there is great value in that type of personal data that can then serve multiple purposes.

Mr. FROST. Why should consumers or people not want their information just available for purchase by the highest bidder?

Professor HU. Well, I think, especially in this instance, it is so critical for us to look at the way in which we do not have a comprehensive system of protection. We have a very siloed system in the United States where we look at all of this individually within its field, but, really, the impact is integrated, and especially with AI technologies, we are going to see an increasing integration.

Mr. FROST. Yes. No, you are 100 percent right. I mean, Congress has failed to deal with this for a long time. How could 23andMe's bankruptcy proceedings lead to the release of people's private genetic information?

Professor HU. Well, I have multiple concerns about whether or not, in the time of bankruptcy, whether the cybersecurity and the data protection protocols will be foremost. And I completely understand the commitments that have been made in the past, and they have been known as a very strong company in their data privacy and cybersecurity protections. But it is a time of chaos when you are in financial duress and when you are now transferring, potentially, the company to others, even if there are promises up front that you carry over those prior commitments, it is really uncertain, and I think that that is why people are panicking.

Mr. FROST. When it comes down to strengthening privacy regulation for our personal data that is held by corporations, what examples can we pull from in terms of state laws?

Professor HU. Well, there are several states now that have very strong data privacy protections, and there are also states that are now leading the way in genetic privacy and biometric information

privacy. And I think that if Congress were to help to understand how best to, you know, bring further protections, strengthening GINA, strengthening HIPAA, then I think that we could get much farther.

Mr. FROST. Are there any approaches that have not been tried yet?

Professor HU. Well, I think that Colorado, for example, with their high-risk AI, you know, Consumer Protection Act, is a model of borrowing from the EU in looking at what types of technologies and what type of AI systems or data-driven systems are going to pose the greatest risk, and I think that is something that Congress could examine.

Mr. FROST. Yes. Genetic research has had lifesaving results, and large amounts of data can only assist in this work, but the loss of data privacy cannot be collateral damage for these breakthroughs and innovation must not mean surrender to corporate control. This is not about one company, but in the battle between people's data, privacy, and corporate profits, the people usually lose. And I hope that both my Democratic and Republican colleagues can agree that it is imperative and past time for Congress to step in on this. Thank you. I yield back.

Mr. HIGGINS. The gentleman yields back. The gentleman from Texas, Mr. Sessions, is recognized for 5 minutes for questioning.

Mr. SESSIONS. Mr. Chairman, thank you very much, and for this hearing today, most interesting on both sides.

Ms. Wojcicki, you and I met on 1/20/2015, up at the Rules Committee. I was Chairman of the Rules Committee at the time and covered much of the things that we are covering today with a different viewpoint, perhaps back then, although we understood that there were Members of the House, soon to be Senate, who did hold very dear thoughts about privacy and the things that would come with that.

I have three questions. The first one is, I assume, for anyone who can answer it, who is going to decide who gets the company? Is it the bankruptcy judge?

Mr. SELSAVAGE. It is first a recommendation from the special committee of 23andMe to evaluate the two final bidders to ensure that there is a highest and best bid for the company. That recommendation will then be presented to the bankruptcy court for the bankruptcy court's evaluation.

Mr. SESSIONS. So, recommendation, and, theoretically, it could be of highest bidder. Is the bankruptcy judge then going to determine the remaining value of what happens in that disposition of the bankruptcy amount?

Mr. SELSAVAGE. It is the bankruptcy court which will determine what happens with the proceeds from the sale, if that is what your question is.

Mr. SESSIONS. Thank you. Anyone disagree with that?

[No response.]

Mr. SESSIONS. Thank you. Data that is being held, I see the term often that might be reserved for the term research. This is used for research. Is there a corresponding value where a person, 23andMe, would ping back a person if they discovered that all of a sudden, something appeared in the marketplace that would correspond to

some DNA markers that then 23andMe recognize, hey, we have a trial. We have an answer. We have dated information. Could we get you to take part in a trial? Is there a moving back from 23andMe to a person that was whose data you had?

Ms. WOJCICKI. Yes. It is a great question. So, we actually call, this was the flywheel, is that when we set out the company, we wanted to create a research platform that was actually what we say, by the people, for the people, so that if the consented customers wanted to go and research a topic, that we could go and all collectively come together, input that information, research it, and then we would actually put that back to customers as a new report.

Mr. SESSIONS. So, this means to me that 23andMe has data and information specific to what might be new research or something that appeared in science, a trial, data, and information where you can link that back to the individual. And I had heard people, perhaps, though, and I could be wrong, this panel say there is no direct link back to a person. Is it based upon if a person opted into that, or do you have it even if someone did not opt in, a way that you could, as part of the service, tell them ten years later, 12 years later, hey, we believe on predictive analysis of what we have learned, you have something on the surface or deep in your DNA, we want you to be aware of something?

Ms. WOJCICKI. So, it is a great question and two very different parts of the service. So, customers have the ability to opt in to research, and in that research part, the scientists are doing discovery.

Mr. SESSIONS. So, they would have had to have opted in in the beginning, and perhaps that was the value of 23andMe. At least it was in 2015 that you and I spoke about.

Ms. WOJCICKI. They have the ability to opt in. We make a discovery. Once we have made a discovery, for instance, we have what is called polygenic risk scores on areas like type 2 diabetes. Once we say we have validated, we have the ability to predict, potentially, who is at higher risk for type 2 diabetes, we turn that into a report. And one of the features of 23andMe as a customer who is buying into the subscription is we continuously update your account with new information as it is coming.

Mr. SESSIONS. So, my point in saying this, and I am sorry to cut you off—I have got about one second left—there is a direct link that with the sale of 23andMe, you would have corresponding data specific to an individual. Thank you very much. I appreciate you being here today. I hope that this stuff is on a website, FAQ, frequently asked questions, or something. There are a lot of people that are here today talking about fear. I think fear is a very negative way to look at things. I think education is. So, I hope you are able to make sure, if you need to update it, that you are looking at that and appropriately answering questions perhaps that Members had today. Mr. Chairman, I want to thank you for the 29 seconds extra. I yield back my time.

Mr. HIGGINS. The gentleman yields. Mr. Crane, the gentleman from Arizona, is recognized for 5 minutes for question.

Mr. CRANE. Thank you, Mr. Chairman. According to public reporting, individuals with Jewish and Chinese heritage were targeted in the hack. It happened a couple of years ago at 23andMe.

Ms. Wojcicki, why were Chinese and Jewish individuals targeted during this hack?

Ms. WOJCICKI. That is a great question. I do not believe it was specifically those individuals. It was definitely something that was reported in the media, and there were a lot of Jewish relatives that were in some of that information, but I do not believe it was necessarily a specific attack on those. It was the credential stuffing.

Mr. CRANE. But didn't one of the individuals say that he would sell information about individuals with Jewish heritage?

Ms. WOJCICKI. They did report that they said that.

Mr. CRANE. Okay. Interesting. Having people's personal DNA profiles unsecured is obviously a very serious issue, could be used to develop bioweapons, force readiness analysis, Black Miller coercion, and pharmaceutical targeting. I noticed when Ms. Pressley asked if you would allow consumers who had submitted their DNA to 23andMe to erase their data from the site before the sale to a new buyer, neither of you could answer yes. I want to go into that for a second. Why could neither of you answer yes, if both of you claim that the end of it, the owners of the DNA, is actually your customers?

Mr. SELSAVAGE. Our customers always have control over their data. You know, basically, they can access their data. They can edit their data. They can opt in or out of any research consent, and most importantly, at any time they so choose to, they can delete their data. In the case of——

Mr. CRANE. Then why can't you answer Ms. Pressley's question that way? Do you remember that question, sir?

Mr. SELSAVAGE. I do not remember the exact question she asked, but for our customers, you know——

Mr. CRANE. Her question, sir, was will you give your customers the ability to opt back in before the sale to a new owner that they did not submit their data to?

Mr. SELSAVAGE. I believe her question to me was will we give people direct notice to say that they can opt in or out of keeping their data. You know, what I am saying today is, at any time, and this has been the case since the founding of 23andMe, that customers can delete their data. It is an automated process. They simply go into their account, like, you know, go to the settings and they can click delete their data. It is an automated process. We delete all their digital data. And if they have biobanked the sample and consented to that, we destroy that sample, and we do that timely, and we have done that for every customer who requested us since, you know, since inception, including the large number of customers who requested deletion of their data since the bankruptcy.

Mr. CRANE. How difficult is it to do that, Mr. Selsavage?

Mr. SELSAVAGE. I think it is very simple. I mean, I think it probably takes somebody less than 5 minutes to go into their account, go to the settings, click "delete my data," and for the company, it is an automated process.

Mr. CRANE. Mr. Selsavage, you said you are very confident that American data will not wind up in the hands of a bad actor. Did you say that a few minutes ago?

Mr. SELSAVAGE. I did, Congressman.

Mr. CRANE. How can you make that claim when seven million users have already had their information stolen?

Mr. SELSAVAGE. Congressman, you know, the cyber incident at 23 was very regrettable, and we have apologized for that to our customers. The data that was actually released in that cybersecurity incident was, you know, mostly DNA relative data, and while it is customer data that was revealed, we believe we have since, you know, enhanced the security at 23andMe where we always maintain that as a top priority for the company. And then second is through the sale process, we are ensuring that the sale of the company will not go to any company that is a foreign adversary to the U.S.

Mr. CRANE. Ms. Wojcicki, did I say that right?

Ms. WOJCICKI. Wojcicki. Yes, right.

Mr. CRANE. Wojcicki, sorry. You said the same thing that you were very confident that data would not wind up in the hands of a bad actor. I mean, you have been in this space for a long time. You know hacks happen every single day. You know that many nation-states that are adversarial to the United States of America have very robust cybersecurity operations. How can you be confident when seven million of your customers have already had their data stolen?

Ms. WOJCICKI. Just to reiterate, I am not part of the bankruptcy process other than the fact that I am an active bidder. During my time at the company, we did very proactive steps, for instance, like I mentioned, keeping the genetic information separate from all the identifiable information. So, we tried to create a structure where even if there was some kind of breach, that you would not be able to reconnect those and identify back to the individuals and who they were. So, in the cyber incident, it was, as Mr. Selsavage was saying, a lot of it was DNA relatives' names and small amounts of information, so it was mostly those names.

Mr. CRANE. Okay. Thank you, Mr. Chairman. I yield back.

Mr. HIGGINS. The gentleman yields. I recognize myself for 5 minutes for questioning.

I think it is important to note, and as America observes this fascinating hearing, that digital data is not secure. You have reports of, according to my research, about 27 percent of Fortune 500 companies have had major data breaches. These are the wealthiest companies, the most advanced security systems. Data breach statistics show a significant increase in both the number of breaches and the number of records exposed within those breaches.

For example, in the United States, the number of data breaches increased from 447 in 2012 to over 3,200 in 2023. In 2023, 353 million individuals were impacted by data compromises, and globally, data breaches exposed over 818 million data sets in the first quarter of 2024. It was intellectually unsound to discuss digital data as if it was secure, and therein lies the problem because, Ms. Wojcicki, 23andMe, congratulations on the success of the company. I am a Republican. I support free enterprise. Glad you had a good run, but let us talk about the issue right now because 23andMe began with a DNA swab, and that swab was sent in to a laboratory, I presume, 23andMe, and that laboratory analyzed that physical data and created a digital file. Is that correct?

Ms. WOJCICKI. Yes.

Mr. HIGGINS. Okay. We are moving quickly. I am just summarizing here for the American people. You send in a swab. It is physical DNA that is received by a laboratory and transitioned to a digital file. At that point, America, no longer secure. And I need to only point to modern history and data breaches and digital theft, but let us move a little bit deeper into this consideration. In these laboratories in 23andMe, did you have Chinese nationals working, ma'am?

Ms. WOJCICKI. So, 23andMe contracted with LabCorp.

Mr. HIGGINS. Yes, did you have Chinese nationals working in laboratories that were processing the DNA physical data and transitioning that data to digital files?

Ms. WOJCICKI. So, Labcorp is a public company. It is one of the largest lab testing——

Mr. HIGGINS. Yes or no. Were there?

Ms. WOJCICKI. I did not control their hiring.

Mr. HIGGINS. Would you believe me when I tell you the answer is yes? Yes, Chinese nationals. Listen to this, America: you sent in your DNA on a swab. No problem. That is cool to check your family history and your family tree, you know. I did it, too, but the expectation of privacy of your digital data was gone the moment you put that thing in the mail, and now Congress has to determine whether or not we are going to allow the abject sale of that data. And let me just say that we are going to draft legislation, Mr. Selsavage. We will draft legislation. I do not know if we will get it right because it is complex. I would estimate there will probably be a dozen different iterations of legislation covering DNA digital data control over the next decade, but Congress must act in response to this newly emerging threat because you are not just talking about 15 million people with 23andMe.

According to my research, over the course of 30 years, 15 million people become 100 million descendants. It is the same basic DNA profile, therefore subject to the same threat of biological weaponization of that DNA profile, and that DNA profile exists in the digital realm where we already acknowledge it is not secure. So, this body is going to create legislation, and that legislation will impact the sale of this data, so both of you have a stake. Quickly, ma'am and sir, advise this body, will you be available for consultation to this Committee as we work through what legislation will look like?

Ms. WOJCICKI. I would be honored to help and participate however I can to help make sure that genetic——

Mr. HIGGINS. However, you can. Thank you, ma'am. Good sir?

Mr. SELSAVAGE. And likewise, I would be happy to help.

Mr. HIGGINS. Professor Hu, we are going to need you. Will you be available?

Professor HU. Absolutely.

Chairman COMER. Thank you. My time has expired. The Chair recognizes Mr. Gill for 5 minutes for questions.

Mr. GILL. Thank you, Mr. Chair.

Mr. HIGGINS. I stand corrected, Mr. Gill. I apologize. Ms. Crockett has arrived. Ms. Crockett is recognized for 5 minutes for questioning. I apologize, Mr. Gill.

Ms. CROCKETT. Thank you so much, Mr. Chair. Despite the messy breakup we all saw unfold last week between the world's richest billionaire and the world's pettiest billionaire, we cannot forget the damage Elon Musk and President Trump have done together to our government, national security, and Americans' privacy. Republicans are holding this hearing acting like they care about protecting your privacy, pretending like their President is not out there trashing privacy and cybersecurity laws to build profiles of Americans' sensitive information that could give him unparalleled power to control what we say and what we do. That is right. Whistleblowers have told the Committee that DOGE is carrying around "backpacks full of laptops to combine protected data from different agencies and that DOGE is not notifying Americans that their data is being moved around even though they are required to do so by Federal law." Professor Hu, why do Federal laws like the Privacy Act and the Federal Information Security Management Act place safeguards around how the Federal government handles and uses Americans' data?

Professor HU. Thank you so much, Congresswoman, for that question. I think that it is absolutely critical to see the urgency of this moment in history, that as we are asking 23andMe to exercise such care and moral obligation to safeguard our national security interests, that we also ask that of our own Federal government and that we look to the laws that we have, such as the Privacy Act and FISMA, as reasons why it is so critical, not only because of the history of potential abuses and misuses that we have seen in the past and also the vulnerabilities that led to the enactment of those laws, but because of the critical national security issues that are emerging, especially in light of AI warfare.

Ms. CROCKETT. Thank you so much. Professor Hu, let me ask you one more question. How does DOGE's haphazard and cavalier handling of American sensitive data present privacy and security risk?

Professor HU. I think that what we really need to understand is that aggregation and that consolidation of data opens us up to a great deal of targeting and also the type of misuse and abuse of that data. And without making sure that we reinforce the systems that we have put in place previously and those specialists and experts that we had hired previously to safeguard those systems, we are really jeopardizing, I think, Americans' privacy.

Ms. CROCKETT. Yes, it seems like we decided to leave all our valuables in the car out where everybody can see it and the door is unlocked. That is what it feels like, but I digress.

Our Federal agencies are tasked with protecting cybersecurity and maintaining critical IT infrastructure that has been gutted by this Administration. Almost a thousand employees were fired or forced out of the Cybersecurity and Infrastructure Security Agency, better known as CISA, weakening America's cyber defenses. Professor Hu, how will these workforce cuts jeopardize our Nation's ability to protect Americans' data from cyberattacks?

Professor HU. Yes. I think that we need to understand the critical role that these agencies and professionals, including CISA, the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, the role that they play in making sure that they safeguard all of our critical infrastructure. And without

the proper staffing, we are throwing ourselves into a great deal of jeopardy. And I think that we also need to recognize the potential conflict of interest here of those that are trying to dismantle these cybersecurity systems.

Ms. CROCKETT. Thank you so much. As another example, Trump's Acting Director of the Consumer Financial Bureau of Protection, which Trump is also trying to unconstitutionally dismantle, recently killed a bill that would have shielded Americans' sensitive information from data brokers. Instead of protecting Americans from companies that sell their address, email, phone number, financial data, political affiliation, religious beliefs, and other sensitive information, Trump is letting them run wild.

I would ask unanimous consent to enter into the record a *Wired* article titled, "CFPB Quietly Kills Rule to Shield Americans From Data Brokers."

Mr. HIGGINS. Without objection, so ordered.

Ms. CROCKETT. Thank you so much. Congressional Democrats and American people are rightfully concerned that their sensitive information is being used, abused, and pulled without regard to our Nation's privacy and information security laws. And we will not forget that just last week, Republicans made us wait more than half an hour while they scrambled to get their Members into this committee room for a hearing that they called yet did not bother to attend because Democrats had the votes to subpoena Elon Musk. If they agree with what Elon has done, why are they so scared to hear from Elon himself? Maybe now that Elon broke up with Donald, the Majority will finally join us in demanding answers from Mr. Musk's time within this Administration.

Let me tell you something. We have seen that this Administration has decided to go after students because of things that they have said. We have seen people get fired because they refused to pledge their loyalty to this daggone cult. This is absurd, and we do not need people being targeted. They are weaponizing us while at the same time making us very vulnerable to those that want to hurt us the most.

Now, listen, I never sent my DNA to anybody, so I do not know where I was stolen from. I am going to tell you right now, I did not do it because I was concerned because there is a history, especially when it comes to Black folks, with taking our stuff. So, I did not do it. So now, I sit here clueless about my heritage. But I tell you that having a hearing on this issue brings about all of those worst fears for me, though, the fact that our data is just out there and our personal biographical information. So, I am just going to ask any and everyone around the science world so that we can make sure that we move forward in this country, when it comes to science, we got to make sure that we are protecting people's information as we are trying to move forward, whether it is AI, whether we are talking about things such as our genes or otherwise. Thank you so much, and I yield. Thank you so much, Mr. Chair.

Mr. Comer [Presiding]. The Chair recognizes Mr. Gill from Texas.

Mr. GILL. Thank you, Mr. Chair, and thank you for holding this hearing on a very important topic, which is data privacy. But I have got a couple of other things that I want to talk about while

we are here, related to this. Ms. Wojcicki, is that how you pronounce it?

Ms. WOJCICKI. Yes, Wojcicki.

Mr. GILL. Wojcicki. Okay. Thank you for being here and taking the time. 23andMe has really, over the past few years, gone out of its way to show how woke it is, and one of the things that it has been promoting, amongst many others, is a variety of different pronouns. Here is a tweet that you guys put out in June 2021. I just want to ask you, what does E mean as a pronoun? It is E.

Ms. WOJCICKI. To be honest, I am not sure.

Mr. GRILL. Okay. Do you know what M means as a pronoun?

Ms. WOJCICKI. I am also not sure.

Mr. GILL. Okay. Don't you think it is important to know what these mean? In this post you wrote, or somebody on your comms team wrote, that using the correct pronouns impacts trans people's health, can reduce the risk of depression and suicide. That is a pretty serious claim. It seems like if you are going to demand people use these pronouns, you would know what they mean, right?

Ms. WOJCICKI. I delegate. 23andMe had a lot of people. We had six, seven people.

Mr. GILL. Right. You were CEO though, right?

Ms. WOJCICKI. I was CEO, but it does not mean I can oversee every single post.

Mr. GILL. Well, this is a very, very politically charged post that you guys put out. I would think that you would have a view on that. Can you tell us what is the difference between ZE and XE? One of them is ZE and one is XE?

Ms. WOJCICKI. I am not up to speed on that.

Mr. GILL. Okay. Does it concern you that not understanding this might increase the risk of depression and suicide amongst trans people?

Ms. WOJCICKI. I support my research team that felt that, you know, it is important for us to be inclusive of everybody and it was very much grounded.

Mr. GILL. I agree, but it does not seem very inclusive if you do not know what they mean, right?

Ms. WOJCICKI. I respect the social team and the research team that put that post together.

Mr. GILL. But you do not know what any of these pronouns mean, but you guys are promoting it?

Ms. WOJCICKI. I assume it is different ways people like to be referred to.

Mr. GILL. What about HIR? What does that mean?

Ms. WOJCICKI. I do not know either.

Mr. GILL. What about FAE/FAER, F-A-E/F-A-E-R.

Ms. WOJCICKI. Again——

Mr. GILL. You would agree these are pretty unusual things, wouldn't you?

Ms. WOJCICKI. I think they represent a lot of the diversity in this country.

Mr. GILL. Okay. I am trying to understand the diversity and I am asking you what they mean. I will give you one more chance. Do you know what ZE, HIR, XE, XEM, FAE, FAER, E, EM mean?

Ms. WOJCICKI. I do not.

Mr. GILL. Okay. Does that concern you that you do not know it? According to your own post here, understanding these and using the correct pronouns would improve your product for trans and non-binary people. It seems like this is directly related to the product.

Ms. WOJCICKI. Again, it was the social team and the research team that felt strongly around putting——

Mr. GILL. Well, you were CEO, so you cannot pawn off responsibility to somebody else here. What about bathroom access? On 23andMe's website—I have got it up here on my phone—there is a 23andMe blog and there is a little subheading about bathroom access. Is it still 23andMe's official position that men should be using women's restrooms?

Ms. WOJCICKI. I am not at 23andMe anymore.

Mr. GILL. Okay. Was it while you were at 23andMe?

Ms. WOJCICKI. I think we had non-gendered bathrooms as well.

Mr. GILL. Well, that is not what this is referring to. This is referring to laws that seek to force, in your own words, force trans individuals to use a restroom that does not correspond to their gender identity. While you were there, was it 23andMe's position that men should be using women's restrooms?

Ms. WOJCICKI. I think our position was just to make sure that we are applicable to laws.

Mr. GILL. This is not in reference. This is actually against laws that would stop people from using the wrong restroom.

Ms. WOJCICKI. Yes.

Mr. GILL. So, this is actually against laws.

Ms. WOJCICKI. I do not have that post in front of me, so I cannot comment specifically.

Mr. GILL. Was it 23andMe's position while you were there that children should be trans'd because that is on this website as well.

Ms. WOJCICKI. I do not know specifically what you are referring to.

Mr. GILL. I can read you a little bit about it: "supports gender-affirming healthcare, such as hormones and surgery for trans youth."

Ms. WOJCICKI. I think 23andMe referred specifically to some of the pediatric guidelines.

Mr. GILL. Sounds to me like you took a genetics company, which you built, and congratulations for doing that, and turned it into a woke social justice organization. You want to run away from that now. It does not sound like you even knew what you were talking about at the time. You do not know what any of these pronouns mean and now realize that this is politically not very popular. It says a lot about where your convictions were and what you meant here. So, thank you, Mr. Chairman.

Chairman COMER. Thank you. And just one last question before we go to a brief closing statement. I am sorry, go ahead.

Mr. MIN. Thank you, Mr. Chair. I just will note that several of our Republican colleagues spent so much time talking about trans, and this is the Oversight Committee. This is a hearing about genetic information. I think it is fair to say that a number of my Republican colleagues seem obsessed with trans issues as opposed to, say, things like the corruption we are seeing in our government,

the illegal removals and deportations of citizens and people here on permanent residence and permanent green cards and student visas.

But this is an important hearing because Americans do deserve to know what the sale of 23andMe will mean for their sensitive genetic data. While 23andMe's privacy policies currently allow customers to delete their data from the company, the next buyer of 23andMe could do away with these types of safeguards for its 15 million customers. Despite today's testimony from the current and former CEO of 23andMe, customers' visibility into their data, where it may be sold, and what the company's third-party partners do with it is extremely opaque.

In addition, it is clear that no comprehensive Federal data exists to limit companies like 23andMe from selling their data to third parties. The collection and storage of copious amounts of sensitive personal information, whether it is in 23andMe's database or in the Federal databases containing Americans' sensitive information, creates a clear target for hostile actors. Sensitive data can be subject to exploitation both for national security purposes, whether it is the CCP, Russia, or other foreign adversaries, or for consumer exploitation, including by data brokers and advertising and market analytics providers.

Our Nation's Federal laws have not kept up with technological advances or the potential threats from malicious and foreign actors. Americans need strong oversight and stronger laws to bolster our national security, our private security, and our privacy protections to make sure that our sensitive data remains safe. If Americans were scared about what 23andMe might do with their data, they would be really scared if they thought about what DOGE and the Trump Administration are already doing with this data. congressional Republicans cannot continue to ignore the Trump Administration's blatant attacks on and destruction of critical security and privacy protections across the government. This Trump Administration has conducted mass terminations of critical Federal IT experts, chief information officers, and other technology professionals, while also removing many of the inspector generals that are meant to ensure good processes. DOGE, meanwhile, has seized unauthorized access of Americans' data, disregarding longstanding cybersecurity practices and existing data privacy laws. And thanks to a brave whistleblower, we know that here on the Oversight Committee, Democrats learned that DOGE is reportedly creating a master database of sensitive information from across all Federal agencies, an apparent violation of existing privacy and cybersecurity protections that ensure that this data cannot be exploited or misused.

But here on this Committee, unfortunately, the Majority is just ignoring this all and sacrificing our rights to data privacy and security all to shield Elon Musk, Donald Trump, and their cronies from accountability. And again, I want to reiterate the fact that so many of our colleagues in this hearing focused on trans issues. They attacked the trans community. I am not sure what that is about when we are talking about privacy. We are faced with real and clear threats to our privacy. This hearing raised some of them, but we ought to be thinking about the threats to our federally held pri-

vacy as well. Congress has to open our eyes and address the threats in front of the American people much better. I yield back.

Chairman COMER. Before I close, Ms. Wojcicki, there are news reports and rumors that Oracle and Executive Chairman Larry Ellison is the backer in your bid to acquire 23andMe. Are you aware of these rumors?

Ms. WOJCICKI. I have read some news reports.

Chairman COMER. Is Oracle the company backing?

Ms. WOJCICKI. The current bid is exclusively from me.

Chairman COMER. Is exclusively what?

Ms. WOJCICKI. Is exclusively from me.

Chairman COMER. All right. So, you are buying your own company out of bankruptcy exclusively?

Ms. WOJCICKI. I am trying very hard.

Chairman COMER. Wow. Very good. Okay. Well, I think that this was a very productive hearing.

I want to thank our witnesses who are here today. I think it is very clear there is bipartisan concern that Americans' sensitive genetic data could end up in the hands of bad actors. We have heard commitment from the two witnesses from 23andMe today that that will not happen. We will be watching that very, very closely. And as the bankruptcy proceeding moves forward and more information is known about the state of the company, then this Committee will continue to conduct its investigation and continue to be transparent with the American people on what we find and do everything in our ability to see that America's private data is protected from bad actors.

So, with that, all Members have five legislative days within which to submit materials and additional written questions for the witnesses, which will be forwarded to the witnesses.

Chairman COMER. If there is no further business, without objection, the Committee stands adjourned. Thank you all.

[Whereupon, at 1:26 p.m., the Committee was adjourned.]