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

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

Prepared Statement of Adam I. Klein

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

Before the U.S. Senate Committee on the Judiciary

June 11, 2025

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

[8] *Id.* § 2(c)(7)(E).

[9] *See id*. § 2(c)(3)(A) ("The term 'data broker' means an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider.").

[10] *See* 28 C.F.R. Part 202; Executive Order 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (Feb. 28, 2024).

[11] *See id.* §§ 202.224 (defining "Human 'omic [sic] data"), 202.303 ("Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in any covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk U.S. sensitive personal data that involves bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived.").

[12] *See* 23andMe, Addressing Data Security Concerns – Action Plan (updated Dec. 5, 2023), https://blog.23andme.com/articles/addressing-data-security-concerns.

[13] *See* Robert Strauss Center for International Security and Law, University of Texas at Austin, *Texas Cyber Clinic*, https://www.strausscenter.org/apply-here-cyber-clinic/.

[14] *See* 28 C.F.R. §§ 202.1001, 1002.

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

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

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

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

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

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

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

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

---

[15] *See* EU Directive 95/46, art. 25; Gen'l Data Protection Reg., arts. 44-45.

[16] *See* Data Protection Comm'n of Ireland, *Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China* (May 2, 2025), https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following.

[17] *See* Testimony of Adam Klein before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, *Protecting Americans' Private Information from Hostile Foreign Powers* (Sept. 14, 2022).

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

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

Intelligence Operations and Transnational Repression

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

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

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

Biomedical Research and AI Models

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

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

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

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

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

Bioweapons

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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