A Continued Pattern of Government Surveillance of U.S. Citizens

James Czerniawski, Senior Policy Analyst: Technology and Innovation, Americans for Prosperity

Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary

U.S. House of Representatives

April 8th, 2025

Dear Chair Biggs, Ranking Member McBath, and Members of the Subcommittee

On behalf of Americans for Prosperity and the millions of activists it represents across all 50 states, we thank you for the opportunity to provide our view on the increasingly problematic and invasive nature of government surveillance of U.S. citizens. In a nation founded on the principles of liberty and limited government, the ever-growing surveillance state is one of the greatest threats to individual freedom. Under the guise of national security, the federal government has overstepped its constitutional limits in empowering and emboldening a national security apparatus that has engaged in warrantless surveillance of Americans with little to no accountability. What began as a program meant for counterterrorism has morphed into a surveillance apparatus that erodes privacy, chills free speech, and undermines faith in key institutions of government critical to protecting Americans.

The revelations of years of numerous documented abuses coupled with a lack of accountability has resulted in an erosion of trust between the American people and the key institutions within government charged with protecting them. At Americans for Prosperity, we believe that national security and constitutionally protected rights are not mutually exclusive. National security should not come at the expense of personal liberties. The intelligence community is bipartisan in its targeting of Americans for surveillance, and it is good to see that Congress is coming together in a bipartisan nature to tackle this critical issue. We hope this hearing can serve as an opportunity to find pathways towards securing bipartisan reforms that can both advance our national security interests and better protect Americans civil liberties.

I. Foreign Intelligence Surveillance Act (FISA) and the Need for Reform

Passed in 2008, Section 702 of the Foreign Surveillance Act granted the government greater powers to conduct warrantless surveillance of suspected foreign terrorists. While this may sound like a reasonable approach to national security, its implementation has often blurred the line between foreign and domestic surveillance. Unfortunately, Section 702 has become a go to resource for the government to access Americans' communications without the proper

protections of a warrant. For example, the Federal Bureau of Investigation (FBI) conducted 200,000 warrantless searches of the communications of American citizens in 2022 alone using the Section 702 data.[1]

The FISA Court revealed how the government had improperly queried the database to spy on people present at the capitol on January 6th, 2021, information on Black Lives Matter protestors in the summer of 2020[2], 19,000 donors to a congressional campaign[3], and targeted elected officials, including a sitting U.S. Senator.[4] These incidents are far outside the scope of Section 702's intended use for foreigners outside of the United States and goes to the heart of the Fourth Amendment and our fundamental natural rights.

Unfortunately, rather than implement appropriate guardrails to ensure they are following the rules, intelligence agencies have failed to implement any meaningful reforms that place privacy at the forefront of policy discussions. Instead, agencies spent time and resources in 2023 issuing a report describing how they were changing their methodology in a way that would decrease the reported number of queries.[5] Essentially, the agencies are seemingly more concerned with the optics of headlines than they are with the sanctity of Americans' privacy and Constitutional protections against overreach and tyranny.

A. The Conversation of Reform

Some proponents of surveillance reform would argue that Congress should let Section 702 authorities expire, however, we feel that would be a grave misstep. Back in 2020, Congress let Section 215 of the PATRIOT Act sunset as they could not come to consensus on which reforms to the program were necessary to keep it in place. An unintended consequence of this outcome was that it did not stop the intelligence agencies from engaging in this type of surveillance. Rather, they simply carried out similar activities under other surveillance authorities like Executive Order 12333, a worse outcome as it comes without the added transparency required under statute coupled with oversight from Congress.

During the most recent reauthorization debate surrounding Section 702, after granting a short-term extension of the authorities in December of 2023 by including it in the must-pass National Defense Authorization Act[6], Congress ultimately reauthorized the surveillance authority under

---

[1] Office of the Director of National Intelligence. Annual Statistical Transparency Report Regarding the Use of National Security Authorities: Calendar Year 2022. 2023, https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.

[2] Sterling, Toby. FBI Misused Intelligence Database in 278,000 Searches, Court Says. Reuters, 19 May 2023, https://www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/.

[3] Foreign Intelligence Surveillance Court. 2021 FISC Certification Opinion. 2021, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.

[4] Carney, Jordain. "FBI Analyst Improperly Searched Surveillance Data for U.S. Senator's Name - Politico." Politico, 21 July 2023, www.politico.com/news/2023/07/21/fbi-surveillance-data-senators-name-00107621.

[5] https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf

[6] Foran, Clair, Fox, Lauren, Grayer, Annie and Haley Talbot. "Defense Policy bill includes short-term extension of controversial government surveillance program". CNN. December 7, 2023. https://www.cnn.com/2023/12/07/politics/ndaa-fisa-extension/index.html

H.R. 7888, the Reforming Intelligence and Securing America Act (RISSA).[7] Proponents of this "solution" argued that it contained meaningful reforms, however, we believe that legislation did little in the form of reforms while simultaneously dangerously expanding the scope of surveillance by changing the definition of what was considered an electronic communications service provider (ECSP).[8]

Those "reforms" largely codified internal guidelines from the FBI, and analysis from the Center for Democracy and Technology found that the FBI conducted an estimated 4,000 queries violating these very guidelines, further reinforcing how insufficient that standard is.[9] While Senator Mark Warner committed to working with colleagues to narrow that definition to address this concern[10], the most recent attempt to do so in the Intelligence Authorization Act was stripped out.[11]

We believe that Congress made serious gains in understanding the necessity for reforms to this surveillance authority, and that this Congress is in a position to build off that momentum with the coming reauthorization of FISA in 2026 to secure serious and meaningful reforms to this program once and for all. While there are many avenues for reform, here are several key areas of reform that Congress should focus on that we would like to highlight, such as:

- **Closing the backdoor search loophole**

  The backdoor search loophole allows for intelligence agencies like the CIA, FBI and NSA to tap into the 702 databases, which is meant to be used to target only non-U.S. persons located overseas, to search billions of international communications to ultimately find and review Americans' phone calls, texts messages and emails. Engaging in such practices explicitly undermines the 4th Amendment rights of Americans. As mentioned earlier, these backdoor searches have been abused to spy on individuals across the political spectrum. According to polling by Demand Progress and FreedomWorks, 76% of Americans believe that government agencies should "obtain warrants before intentionally searching international communications obtained without a warrant for conversations involving people in the US."[12] During the reauthorization debates, amendments were put forward that sought to strike a balance that would accommodate legitimate security needs, such as exigent circumstances, certain cybersecurity-related queries, and consent queries, where queries are performed merely for identification or aiding of potential victims. Such a warrant requirement wouldn't be necessary for searches of metadata, thus allowing the FBI the flexibility to determine whether U.S.

[7] U.S. Congress. (2024). H.R. 7888 – Reforming Intelligence and Securing America Act. 118th Congress. Retrieved from https://www.congress.gov/bill/118th-congress/house-bill/7888/text
[8] Id.
[9] Laperruque, Jake. "Requiring a Warrant for U.S. Person Queries Is Critical for FISA 702 Legislation." Center for Democracy & Technology. 25 Mar. 2024, https://cdt.org/insights/requiring-a-warrant-for-u-s-person-queries-is-critical-for-fisa-702-legislation/.
[10] https://www.congress.gov/118/crec/2024/04/18/170/68/CREC-2024-04-18-pt1-PgS2837.pdf
[11] Matishak, Martin. "No FISA fix in annual intelligence policy bill approved by House panel". The Record. June 12th, 2024. https://therecord.media/house-intel-committee-approves-bill
[12] https://demandprogresseducationfund.org/new-polling-as-mass-surveillance-debate-reaches-final-stages-in-congress-americans-demonstrate-overwhelming-support-for-increased-privacy-protections/.

persons are in contact with foreign targets.

- **Closing the Data Broker Loophole**

  Congress should continue to push for reforms to prevent the government from being able to circumvent Americans' constitutional rights by purchasing their personal data from private actors without a warrant. The purchase of such information by the government creates an additional threat, as law enforcement can then use this data tied to Americans engaging in constitutionally protected activities and subject them to additional surveillance via other technologies. Coupled with the backdoor search loophole, these end runs around the Fourth Amendment naturally have a chilling effect on the free speech rights of millions of Americans as they would fear being subjected to unwarranted government spying. Similar to the backdoor search loophole, Americans strongly agree with this proposal. According that same polling, 80% of Americans agree that government agencies should "obtain warrants before purchasing location information, internet records, and other sensitive data about people in the U.S. from data brokers."[13] The Fourth Amendment is Not for Sale Act, which passed the house this past Congress, offers a real solution to tackling this precise problem.

- **Strengthening third-party oversight at the FISA Court**

  Congress should expand the role of neutral, third-party attorneys – or amici – within the FISA Court processes as additional scenarios arise that threaten Americans' rights. Congress should consider requiring FISA Court judges to appoint amicus curae to cases with "sensitive investigative matter" as long as the court doesn't find it to be inappropriate. For example, if the court feels that appointing an amicus could jeopardize an ongoing investigation or reveal sensitive methods, it can choose not to do so. Furthermore, an amicus should be able to raise issues with the FISA Court at any time and give both the court and the amicus access to document and information related to the surveillance application. This would be a significant improvement to due process and increase civil liberties protections for Americans at the courts by ensuring that decisions about surveillance didn't happen entirely in secret without any counterarguments or checks. Congress considered this issue in the past, when the Senate voted to adopt the Lee-Leahy amendment with overwhelmingly strong bipartisan support with a vote of 77-19 to the USA Freedom Act. During the most recent FISA reauthorization debate, the Government Surveillance Reform Act included a section based on that very amendment.

It's important to note that key reforms such as these will not end any surveillance authorities or prevent them from being used to ensure national security, but they will play a critical role in ensuring that the rights of American citizens aren't trampled on in the process.

II. Government's use of Technology for Surveillance

[13] Id.

The government is no stranger to utilizing technology to aid in its mission of public safety. Technology is an incredibly powerful tool in the hands of law enforcement, as it can aid with their duties surrounding crime prevention, investigation and response. However, without proper guardrails, they are ripe for abuse in ways that undermine the communities' trust in them, running directly against their public safety mission.

For example, Facial recognition is a powerful technology that in a commercial setting can provide some benefits for users, but in the hands of government presents some highly problematic questions.

While facial recognition technology is older than perhaps people may realize, dating back to the 1960s when Woodrow Bledsoe developed a semi-automated facial recognition system to analyze facial features within an image[14], the technology itself has experienced rapid gains in recent years. While the technology is impressive, it's still imperfect and can needlessly place innocent people in the crosshairs of law enforcement. A federal study in 2019 showed that Asian and African American people were up to 100 times more likely to misidentified than white men, depending on the algorithm and what type of search was conducted. According to that same study, Native Americans had the highest false positive rate of all ethnicities.[15]

At the state level, Robert Williams presents a case study of what happens when law enforcement becomes overly reliant on technology. In January of 2020, police in Detroit used facial recognition technology on low quality video from security cameras in the store, which produced Mr. Williams' name. Police admitted that their use of facial recognition technology was what prompted them to arrest Williams in front of his family. Ultimately, the charges against Williams were dropped, but not before he had spent 30 hours in jail and had to make bail for a crime he didn't commit.[16] Congress should continue to work to explore ways to implement common sense restrictions around the use of such technologies by law enforcement while still allowing the technology to develop so that it can be an effective tool to advance public safety in the future.

While Artificial Intelligence is a relatively new topic of discussion in Congress, its use cases in this space aren't exactly new. The intelligence community has leveraged artificial intelligence in its surveillance practices to help analysts sift through the vast amounts of intercepted communications.[17]

Predictive Policing, which uses machine learning algorithms, analyzes large datasets to predict where and when crimes are likely to occur. In Florida, one such program came under fire after

---

[14] Jeremy Norman. "Woodrow Bledsoe Originates of Automated Facial Recognition." Jeremy Norman's History of Information. December 30, 2020. http://www.historyofinformation.com/detail.php?entryid=2495.

[15] Drew Harwell. "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use." Washington Post. December 19, 2019. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[16] Bobby Allyn. "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest of Black Man." NPR. June 24, 2020. https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

[17] Christopher R Moran, Joe Burton, George Christou, The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying, Journal of Global Security Studies, Volume 8, Issue 2, June 2023, ogad005, https://doi.org/10.1093/jogss/ogad005

investigative reporting revealed how the program being utilized there led to months of harassment under the guise of a "prolific offender check".[18] The program was so problematic that the county unsurprisingly got sued by the Institute for Justice, ultimately settling and admitting that the program had repeated constitutional violations.[19]

Congress should explore ways to ensure there are guardrails around law enforcement use by executive agencies and work with their state counterparts to ensure similar efforts are taken up there.

Lastly, recent revelations around the bankruptcy announcement for 23andMe present interesting questions about biometric privacy.[20] The announcement sent shockwaves through the ecosystem, driving a surge in website traffic as customers rushed to the website looking for details around deleting data and closing their accounts.[21] The company has roughly 15 million customers around the globe.[22] FTC Chair Andrew Ferguson understands some of the privacy concerns presented here, recently issuing a letter stating that the promises made by 23andMe must be kept by whomever ultimately purchases that information.[23] However, there is a risk that the sensitive type of data held by 23andMe could potentially get funneled to the government via the data broker loophole, allowing for a massive expansion of genetic surveillance to empower governments to go on what amounts to a genetic fishing expedition. At a minimum, it's definitely a topic that the subcommittee and the committee more broadly should potentially explore.

III. Conclusion

Keeping Americans safe is a laudable goal and one we strongly support. It is impossible to ignore that we live in a dangerous world and that there are powers that seek to do harm against the United States. We appreciate the work of the dedicated individuals at these agencies trying to protect us from those dangers. However, that mission of public safety can't come at any expense or without considering other tradeoffs. As we have repeatedly said, protecting our constitutional rights and national security are not mutually exclusive goals. We appreciate the work of this subcommittee and the Judiciary Committee as a whole in trying to pursue the critical and needed

---

[18] McGrory, Kathleen, et al. "A Futuristic Data Policing Program Is Harassing Pasco County Families." Pasco's Sheriff Created a Futuristic Program to Stop Crime before It Happens. It Monitors and Harasses Families. | Investigations | Tampa Bay Times. https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/

[19] Institute for Justice. Case Closed: Pasco Sheriff Admits Predictive Policing Program Violated Constitution. 22 Feb. 2023, https://ij.org/press-release/case-closed-pasco-sheriff-admits-predictive-policing-program-violated-constitution/.

[20] 23andMe. Questions Related to 23andMe's Chapter 11 Filing. March 26, 2025. https://customercare.23andme.com/hc/en-us/articles/30805135934615-Questions-related-to-23andMe-s-Chapter-11-Filing.

[21] Williams, Kevin. "23andMe bankruptcy: With America's DNA put on sale, market panic gets a new twist." CNBC.com. March 30, 2025. https://www.cnbc.com/2025/03/30/23andme-bankruptcy-selling-deleting-dna-genetic-testing.html

[22] Id.

[23] Ferguson, Andrew. "Re: In re 23andMe Holding Co., et al., Case No. 25-40976, United States Bankruptcy Court for the Eastern District of Missouri (Eastern Division)." Federal Trade Commission. March 31, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/23andme-letter-ferguson.pdf

reforms to curb the pattern of continued surveillance of U.S. citizens. It builds upon the committee's admirable and uniquely bipartisan efforts to reform surveillance abuses last year, reflecting the overwhelming and bipartisan demand from the public for strong privacy protections from government predations, something we wish to see continue this Congress. We stand ready to work with you and look forward to answering any questions you may have.