Congress of the United States
Washington, DC 20515

September 4, 2024

President Joseph R. Biden, Jr.
Vice President Kamala D. Harris
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500

Dear President Biden and Vice President Harris:

Earlier this month, reports emerged that hackers have stolen and leaked sensitive personal records of 2.9 billion people, including potentially all Americans.[1] Given the security implications of this extraordinary data breach, we urge your administration to investigate the incident and provide the American public with answers as to how this hack occurred, how the relevant data brokers will be held accountable, and to what extent the government's continued investment in the data broker ecosystem contributed to this catastrophic data breach and the entities responsible.

We also demand your endorsement of legislative solutions limiting government purchases from data brokers and halting the government's purchase of hacked data. These payments to data brokers amount to the government's ongoing subsidization of the data broker industry. Americans should not have to fear bad actors will abuse their hacked data or that their own government will purchase their data, wittingly or not, in circumvention of their civil liberties.

The federal government must reconcile its interest in safeguarding our constituents' personal data with its demand for warrantless access to the same kind of sensitive personal data on Americans sold by data brokers, which is helping fuel an industry predicated on surveilling virtually everyone in the country. As recently as this year, your administration has instead forcefully opposed overwhelmingly popular and bipartisan privacy protections like the Fourth Amendment Is Not For Sale Act.[2] This bill would bar the unconscionable practice of funneling taxpayers' money to data brokers. The privacy of our constituents, as citizens and consumers, must be protected.

---

[1] Jon Healey, *Hackers may have stolen the Social Security numbers of every American. Here's how to protect yourself*, LOS ANGELES TIMES (Aug. 13, 2024), https://www.latimes.com/business/story/2024-08-13/hacker-claims-theft-of-every-american-social-security-number (last visited Sep. 4, 2024).

[2] *New polling: As mass surveillance debate reaches final stages in Congress, Americans demonstrate overwhelming support for increased privacy protections*, DEMAND PROGRESS EDUCATION FUND (Dec. 14, 2023), https://demandprogresseducationfund.org/new-polling-as-mass-surveillance-debate-reaches-final-stages-in-congress-americans-demonstrate-overwhelming-support-for-increased-privacy-protections/ (last visited Sep 4, 2024).

The recently exposed personal data, which was reportedly released in unencrypted form on a hacking forum, appears to include full names, dates of birth, Social Security numbers, addresses, and phone numbers.[3] According to a new class action lawsuit against National Public Data, the reported source of the leaked information, the data also includes people's address histories spanning at least three decades and information about family members and relatives.[4]Other data for sale includes even more sensitive information, including people's location, political and religious interests, and far more.[5]

We are especially concerned that this data could enable malicious actors to build a sophisticated dossier on every American that can cross-reference and validate other sensitive personal data obtained from the largely unregulated data broker industry, as well as other past and future data breaches — such as the recent theft of genetic data and family tree history from 23andMe and the hacking of government employees' security clearance records retained by the Office of Personnel Management.[6][7] Moreover, this data breach is alleged to have occurred in April 2024, which means the hackers had four months to mine, sell, and otherwise exploit the data in the shadows before the American public was broadly alerted to the theft. This is unacceptable.

The resulting security risks must also account for the reality that certain Americans, by virtue of their roles, responsibilities, or relationships, are highly attractive targets for foreign adversaries and other malicious entities with ill intent towards the United States. That list of potential targets runs the gamut: lawmakers and their aides, federal agency officials, law enforcement agents, diplomats, military personnel, political party leaders, contractors and employees with a security clearance granting them access to classified information, journalists and media platform owners, and operators of critical infrastructure like power plants, internet backbones, and drinking water systems. As a result of the National Public Data breach, the basic

---

[3] Kris Holt, *Hackers may have leaked the Social Security numbers of every* American, ENGADGET (Aug. 13, 2024), https://www.engadget.com/cybersecurity/hackers-may-have-leaked-the-social-security-numbers-of-every-american-150834276.html (last visited Sep 4, 2024).

[4] Class Action Complaint and Demand for Jury Trial at 6-7, Hofmann v. Jerico Pictures, No. 24-CV-61383 (S.D. Fla. Aug. 1, 2024).

[5] Justin Sherman, *Data brokers and sensitive date on U.S.* individuals, TECH POLICY AT SANFORD (2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf (last visited Sep 4, 2024).

[6] Lorenzo Franceschi-Bicchierai, *23andMe confirms hackers stole ancestry data on 6.9 million users*, TECHCRUNCH (Dec. 4, 2023), https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/ (last visited Sep 4, 2024).

[7] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, COMMITTEE ON OVERSIGHTS AND GOVERNMENT REFORM (Sept. 7, 2016), https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf (last visited Sep 4, 2024).

personal information of these Americans may have been exposed and made readily available to those who seek harm upon the United States.

We ask for a swift and comprehensive response from your administration, including acknowledgement of the severe consequences of this breach for our national security — and for the executive branch to finally join us, hundreds of our colleagues, and hundreds of millions of Americans in demanding an end to the federal government's subsidizing and warrantless exploitation of data broker surveillance.

Sincerely,

Andy Biggs
Member of Congress

Warren Davidson
Member of Congress

Jeff Duncan
Member of Congress

Randy Weber
Member of Congress

Ralph Norman
Member of Congress

Andy Ogles
Member of Congress

Paul A. Gosar D.D.S.
Member of Congress

Barry Moore
Member of Congress

Ben Cline
Member of Congress