

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE,

ET AL.,

Plaintiffs,

v.

PRESIDENTIAL ADVISORY COMMISSION ON
ELECTION INTEGRITY,

ET AL.,

Defendants.

No. 1:17-cv-01398, Hon. Royce C.
Lamberth

**BRIEF OF FORMER NATIONAL SECURITY AND TECHNOLOGY
OFFICIALS AS AMICI CURIAE SUPPORTING PLAINTIFFS'
MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTION TO
DISMISS**

JOSHUA A. GELTZER (D.C. Bar No. 1018768)
INSTITUTE FOR CONSTITUTIONAL ADVOCACY
AND PROTECTION
Georgetown University Law Center
600 New Jersey Ave. NW
Washington D.C. 20001
Telephone: 202.661.6728
JG1861@Georgetown.edu

ROBERT S. LITT*
DAVID A. NEWMAN*
SOPHIA M. BRILL*
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue N.W.
Washington, D.C. 20006

ROBERT TAJ MOORE*
MORRISON & FOERSTER LLP
250 West 55th Street
New York, New York 10019

Counsel for Amici Curiae

* *pro hac vice* motions pending

TABLE OF CONTENTS

TABLE OF CONTENTS..... i

TABLE OF AUTHORITIES ii

INTEREST OF AMICI CURIAE..... 1

INTRODUCTION 2

ARGUMENT 3

I. THE COMMISSION’S AGGREGATION OF SENSITIVE VOTER DATA AND ITS STORAGE OF THAT DATA AT THE WHITE HOUSE CREATES SUBSTANTIAL CYBERSECURITY VULNERABILITIES 3

 A. Aggregating Vast Amounts Of Personal Data Poses A Substantial Risk For Cyberattacks 3

 1. Large-scale databases containing personal information are particularly attractive targets for malicious cyber actors 3

 2. The Commission’s database would likely be targeted by hostile nation-states seeking to interfere in U.S. elections 6

 3. The Commission’s database could also be targeted by criminal actors seeking to sell personal data for profit 11

 B. Storing Sensitive Personal Data on White House Systems Introduces Heightened Vulnerabilities 12

II. THE COMMISSION’S CREATION OF THIS DATABASE RUNS CONTRARY TO THE PURPOSES OF THE PRIVACY ACT AND COULD CAUSE SIGNIFICANT ONGOING HARM..... 17

 A. The Commission’s Conduct Runs Counter To The Privacy Act’s Purpose Of Ensuring That Personal Data Handled By The Federal Government Receives Appropriate Protections..... 17

 B. The Commission’s Aggregation Of This Data Could Cause Ongoing Harms That Would Be Difficult To Remedy..... 20

CONCLUSION..... 21

APPENDIX: LIST OF AMICI CURIAE 22

CERTIFICATE OF SERVICE 23

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Am. Civil Liberties Union v. Dep’t of Justice</i> , 655 F.3d 1 (D.C. Cir. 2011).....	6
<i>Attias v. CareFirst, Inc.</i> , 865 F.3d 620 (D.C. Cir. 2017).....	11
<i>Ctr. for Nat’l Sec. Studies v. Dep’t of Justice</i> , 331 F.3d 918 (D.C. Cir. 2003).....	6
<i>Doe v. Dep’t of Justice</i> , 660 F. Supp. 2d 31 (D.D.C. 2009).....	19
<i>Remijas v. Nieman Marcus Group, LLC</i> , 794 F.3d 688 (7th Cir. 2015).....	11
<i>United States v. Dokuchaev</i> , No. 3:17-cr-103 (N.D. Cal. Feb. 28, 2017).....	10
<i>United States v. Ferizi</i> , No. 1:16-cr-42 (E.D. Va. June 15, 2016).....	12
Statutes	
5 U.S.C. § 552a.....	17, 18
Executive and Congressional Materials	
Exec. Order No. 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (May 11, 2017).....	14
“Federal Information Security Modernization Act of 2014: Annual Report to Congress for Fiscal Year 2016”.....	13
GAO, “Cybersecurity: Actions Needed to Strengthen U.S. Capabilities” (Feb. 2017).....	13
GAO, “Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System” (Jan. 2016).....	13

“Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections” (Jan. 6, 2017).....6, 7, 8

Memorandum from Jonathan R. Cantor, “DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information” (Apr. 27, 2017).....19

S. Rep. No. 93-1183 (1974).....18

Seena Gressin, “The Equifax Data Breach: What to Do,” Federal Trade Commission (Sep. 8, 2017)4

Statement of Adm. Michael S. Rogers, Commander, United States Cyber Command, before the Senate Comm. on Armed Services (May 9, 2017)9

Statement of James R. Clapper before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism (May 8, 2017).....10

Testimony of Colin Stretch before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism (Oct. 31, 2017)7

Transcript, “Cybersecurity: Ensuring the Integrity of the Ballot Box,” Hrg. before the House Comm. on Oversight and Gov’t Reform, Subcomm. on Information Technology (Sept. 26, 2016)9

Transcript, “OPM: Data Breach,” Hrg. before the House Comm. on Oversight and Gov’t Reform (June 16, 2015).....20

United States Computer Emergency Readiness Team, “Securing Voter Registration Data” (last revised Sept. 30, 2016).....5, 17

Video Recording, Hrg. before the Senate Comm. on Homeland Security and Governmental Affairs (Sept. 27, 2017)10

Video Recording, Hrg. before the Senate Select Comm. on Intelligence (Nov. 1, 2017)7

Other Authorities

Associated Press, “How States Are Handling Trump’s Voter Information Request” (Aug. 2, 2017)20

Brendan Pierson, “Anthem to Pay Record \$115 Million to Settle U.S. Lawsuits Over Data Breach,” *Reuters* (June 23, 2017).....4

Brian Bennet & W.J. Hennigan, “China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say,” *Los Angeles Times* (Aug. 31, 2015).....10

Daisuke Wakabayashi & Scott Shane, “Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election,” *N.Y. Times* (Sept. 27, 2017)7

Dell Cameron, “Even a Novice Hacker Could Breach Network Hosting Kris Kobach’s Bogus Voter Fraud Program,” *Gizmodo.com* (Nov. 9, 2017)17

Demetri Sevastopvlo, “Chinese Hack Into White House Network,” *Financial Times* (Nov. 6, 2008)16

Devlin Barrett & Siobhan Gorman, “Gmail Hack Targeted White House,” *Wall St. J.* (June 3, 2011).....16

Ellen Nakashima, “Hackers Breach Some White House Computers,” *Wash. Post* (Oct. 28, 2014)16

George R. Lynch, “Website Creating Company Faces Data Breach Affecting Over 40 Million Users,” *Bloomberg BNA* (Oct. 24, 2016).....4

Jaikumar Vijayan, “The Identity Underworld: How Criminals Sell Your Data on the Dark Web,” *Christian Science Monitor* (May 6, 2015).....11

Jennifer Martinez, “White House Thwarts Hacker Attack on Unidentified Computer System,” *The Hill* (Oct. 1, 2012)16

Jessica Huseman & Derek Willis, “The Voter Fraud Commission Wants Your Data—But Experts Say They Can’t Keep It Safe,” *ProPublica*, (Oct. 23, 2017)17

Lillian Ablon, et al., *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation (2014).....11

Michael Chertoff, “Trump’s Voter Data Request Poses An Unnoticed Danger,” *Wash. Post* (July 15, 2017)13

Michael Shear, “Technology Upgrades Get White House Out of the 20th Century,” *N.Y. Times* (Apr. 3, 2016).....15

Sari Horowitz, et al., “DHS Tells States About Russian Hacking During 2016 Election,” *Wash. Post* (Sept. 22, 2017).....9

Sasha Issenberg, *The Victory Lab: The Secret Science of Hidden Campaigns* (2013).....6

Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” *N.Y. Times* (Nov. 1, 2017)7

Taylor Hatmaker, “Exposed GOP Database Demonstrates the Risks of Data-Hungry Political Campaigns,” *TechCrunch* (June 19, 2017)8

INTEREST OF AMICI CURIAE

Amici curiae are former national security and technology officials who have a wealth of experience combatting cyber threats posed by foreign adversaries and other malicious actors.¹ Amici have worked at senior levels in administrations of both parties and share strong concerns about securing the integrity of our nation's electoral systems. This brief is intended to highlight for the Court a particular aspect of this litigation that has been referred to but not substantially discussed by either party: the potentially serious national security and cybersecurity implications of the Presidential Advisory Commission on Election Integrity's compilation of a massive database of personally identifiable information about American voters and its storage of that database on White House systems. Amici are uniquely positioned to provide the Court with information and insight about the risks that such a database could be breached, as well as the potential consequences of such a breach.

¹ No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici curiae, their members, or their counsel made a monetary contribution to the preparation or submission of this brief.

INTRODUCTION

Americans recently witnessed an unprecedented attack against our democracy by a hostile nation-state that sought to influence the outcome of our elections. Numerous current and former national security officials and cybersecurity experts have highlighted the urgent need to prevent similar activities—or worse—from occurring in the next election cycle. Our election infrastructure is a continuing target for foreign adversaries, including Russia, and these adversaries are capable of, and increasingly intent on, waging sophisticated cyber campaigns against core U.S. democratic institutions.

The stated mission of the Presidential Advisory Commission on Election Integrity (the “Commission”) is to ensure the integrity of our electoral systems. But given the advanced cyber threats posed by foreign adversaries, there is a serious risk that the Commission’s activities will ultimately make U.S. election systems more susceptible to compromise and abuse. The Commission has aggregated and continues to aggregate large volumes of data about American voters, including names, addresses, partial social security numbers, and voting history, into one centralized database stored, operated, and maintained by the White House. That database may be a compelling target for foreign adversaries seeking to interfere in future elections through a variety of means, as well as for cyber criminals and other malicious actors. Yet, despite this grave vulnerability, the Commission chose to move the database from a network administered by the Department of Defense to an ad hoc system built by White House personnel. *Amici*, who have a wealth of experience as national security and cybersecurity officials, have authored this brief in order to highlight the substantial risks that assembling and maintaining such a database could create.

For all of the vulnerabilities demonstrated during last year’s elections, one feature of our state-based election system that poses challenges to would-be attackers is the extent of its

decentralization—including the degree to which information that could be used to exploit potential vulnerabilities is widely dispersed across numerous systems, formats, and regions. That strength is critically undermined by the Commission’s conduct and will continue to be undermined so long as the Commission’s database is maintained. Because the Commission’s maintenance of this database could enable malicious actors to inflict significant harms on the nation’s electoral process as well as on individual voters, *amici* seek to inform the Court’s understanding of these potential harms as it evaluates Plaintiffs’ complaint and the Government’s motion to dismiss.

ARGUMENT

I. THE COMMISSION’S AGGREGATION OF SENSITIVE VOTER DATA AND ITS STORAGE OF THAT DATA AT THE WHITE HOUSE CREATES SUBSTANTIAL CYBERSECURITY VULNERABILITIES

By aggregating large volumes of personal data in one centralized location, the Commission has created and continues to maintain a compelling target for foreign adversaries and other malicious actors. Personally identifiable information (“PII”) about millions of American voters would be extremely valuable to foreign adversaries seeking to interfere in future elections. This data would also be a valuable target for criminal organizations seeking to steal it for purposes of identity theft or to sell on the black market. Moreover, the Commission has compounded these risks by hosting the database on a White House system that has never been used to store information of this kind and may lack core safeguards.

A. Aggregating Vast Amounts Of Personal Data Poses A Substantial Risk For Cyberattacks

1. Large-scale databases containing personal information are particularly attractive targets for malicious cyber actors

A database that contains large volumes of PII is an extremely attractive target for cyberattacks. Hackers seek to exploit this type of information for a number of reasons, ranging

from ordinary criminal profiteering (e.g., to commit identity theft or to sell the information on the black market for others to commit identity theft) to intelligence collection by hostile nation states or non-state actors. The bigger the database, the greater the payoff from a potential breach.

A large database aggregating PII of millions of American voters in one place, as the Commission has compiled and continues to compile, would constitute a treasure trove for malicious actors. One need only examine some of the most recent high-profile data breaches to understand the extent to which information of this nature is regularly targeted by a wide range of actors and the potential harm that could ensue from a breach. The recent attack against Equifax, for example, compromised the information of up to 143 million people, including their names, addresses, dates of birth, credit card information, social security numbers, and driver's license numbers.² Major breaches against health care providers and retail companies have demonstrated similar patterns. For example, the 2015 Anthem breach compromised names, birth dates, social security numbers, e-mail addresses, and income information of a reported 79 million people.³ In 2016, Weebly, a web-hosting service, experienced a hack that exposed the IP addresses, usernames and/or e-mail addresses, and hashed passwords of some 43 million users.⁴ Government databases with large volumes of PII have also been the subject of significant

² Seena Gressin, "The Equifax Data Breach: What to Do," Federal Trade Commission (Sept. 8, 2017), available at <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>.

³ Brendan Pierson, "Anthem to Pay Record \$115 Million to Settle U.S. Lawsuits Over Data Breach," *Reuters* (June 23, 2017), available at <https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML>.

⁴ George R. Lynch, "Website Creating Company Faces Data Breach Affecting Over 40 Million Users," *Bloomberg BNA* (Oct. 24, 2016), available at <https://www.bna.com/website-creating-company-b57982079041/>.

breaches—including the infamous breach of the federal Office of Personnel Management, which resulted in the theft of highly sensitive information about more than 20 million Americans.

The proliferation of such attacks poses profound challenges to many facets of our election system. The Department of Homeland Security has warned that “[v]oter registration databases present a unique target for cyber threat actors” and that “[i]t is vital that security professionals take precautions to defend [these systems] against intrusion.”⁵ The information that the Commission has requested and continues to aggregate contains basic PII such as names, addresses, and dates of birth, as well as more sensitive information such as partial social security numbers, voting history, criminal records, and military status. *See* Pls.’ Amended Compl. ¶ 62, ECF No. 21 (describing information requested by the Commission); Pls.’ Opp. to Mot. to Dismiss Exh. G-2, at 8-9, ECF No. 30 (listing various states that have provided data to the Commission).⁶ Even if some of this information may already be publicly available, it becomes far more valuable to malicious actors when centralized and combined with other public and non-public information.

That risk is particularly grave in the event that the data is acquired by hostile nation-states, which may be capable of culling through large volumes of information and combining that information with data already in their possession in order to assemble more comprehensive files about American citizens for espionage and counter-intelligence purposes. As the Court of Appeals for the D.C. Circuit has noted in the context of national security information, new disclosures of information must be viewed in light of a broader “mosaic” because “[w]hat may

⁵ United States Computer Emergency Readiness Team, “Securing Voter Registration Data” (last revised Sept. 30, 2016), available at <https://www.us-cert.gov/ncas/tips/ST16-001>.

⁶ Copies of the underlying letters from the Commission’s Vice Chair, Kris W. Kobach, seeking information from all 50 states and from the District of Columbia are available at <https://www.whitehouse.gov/sites/whitehouse.gov/files/docs/information-requests-to-states-06282017.pdf>.

seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.” *Ctr. for Nat’l Sec. Studies v. Dep’t of Justice*, 331 F.3d 918, 928 (D.C. Cir. 2003) (quoting *CIA v. Sims*, 471 U.S. 159, 178 (1985)) (alterations in original); *see also Am. Civil Liberties Union v. Dep’t of Justice*, 655 F.3d 1, 9 (D.C. Cir. 2011) (“an individual’s privacy interest in limiting disclosure or dissemination of information does not disappear just because it was once publicly released” (citing *Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 762-63 (1989))). In recent years, electoral politics and campaigning have been transformed by the trend toward intensively compiling and mining seemingly innocuous bits of user data—including the very types of data that the Commission seeks to ingest—in search of hidden insights about voter behavior.⁷ This trend has not gone unnoticed by America’s sophisticated foreign adversaries.

2. *The Commission’s database would likely be targeted by hostile nation-states seeking to interfere in U.S. elections*

The 2016 election cycle teaches a critical lesson: American voters and the integrity of our election systems are targets for hostile nation-states. By interfering with our nation’s electoral process, foreign adversaries can seek to undermine not only particular candidates but also our democracy as a whole. That was Russia’s clear goal in 2016. The United States Intelligence Community concluded unanimously that “Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election.” “Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections,” at ii (Jan. 6, 2017) (“ICA”).⁸ This influence campaign “followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government

⁷ *See generally* Sasha Issenberg, *The Victory Lab: The Secret Science of Hidden Campaigns* (2013) (discussing rising use of data analysis in political campaigns).

⁸ Available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’”

Id.

The ICA highlights multiple aspects of Russia’s influence campaign, including its hacking and leaking of e-mails, its intrusions into state and local electoral boards, and its social media efforts that sought to drive propaganda. ICA at 2-4. News reports continue to shed light on these social media efforts, and Congress has recently heard testimony about Russia’s extensive efforts to purchase advertising, to maintain fake social media accounts and “troll farms,” and to target particular types of voters.⁹

Voter targeting efforts, in particular, could benefit from access to the types of information maintained by the Commission. Armed with names, addresses, and voting histories—including information about individuals’ party registration and frequency of voting—a foreign adversary such as Russia could conduct targeted information campaigns against particular subsets of voters. It could even seek to undermine voters’ access to the polls by, for example, targeting individuals of one party or another (or perhaps of all parties) with disinformation about the locations or hours of polling places or false reports that an election has been postponed or

⁹ Video Recording, Hrg. before the Senate Select Comm. on Intelligence at 00:53:09 – 00:57:20 (Sen. Richard Burr describing how “Russia trolls” created two competing Facebook groups that encouraged “both sides to battle in the streets,” a tactic intended to create “divisions between real Americans.”), available at <https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections>; Testimony of Colin Stretch before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism, at 6 (Oct. 31, 2017) (stating that approximately 126 million people may have seen Russian-sponsored content on Facebook between 2015 and 2017), available at <https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf>; Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” *N.Y. Times* (Nov. 1, 2017), available at https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html?_r=0; Daisuke Wakabayashi & Scott Shane, “Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election,” *N.Y. Times* (Sept. 27, 2017) (describing Russia’s use of fake Twitter accounts to influence the 2016 elections and to continue sowing political and social discord since), available at <https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html>.

canceled. In short, a national database containing this type of information constitutes a particularly attractive target for Russia or other adversaries seeking to conduct these types of hostile activities. Even if it is correct that some of the information is available in disparate locations and formats across the United States, such as in states' voter registration records or in political parties' databases, and indeed even if private actors, such as the Republican and Democratic National Committees, have reportedly already attempted to compile a wide range of data on American voters—an effort that may have itself created vulnerabilities¹⁰—the Federal Government should be seeking ways to mitigate those risks, not to compound and exacerbate them. Aggregating a comprehensive and official set of such data onto one high-profile, widely publicized server maintained by the White House may reduce the technical and practical barriers to a foreign adversary acquiring such information and making use of it without detection.

Additionally, if a foreign adversary or other malicious actor were capable of *altering* the information contained in the database, the results could have other serious implications for future elections. To choose one example, an adversary could manipulate records to create phony irregularities (such as by altering social security numbers or criminal histories) in the hopes of spawning baseless inquiries and investigations that could result in the wrongful removal of legitimate voters from registration rolls. The events of 2016 demonstrate that Russia did in fact target voter registration rolls as part of its active measures campaign. The Intelligence Community concluded that “Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards”—though they did not access systems involved in vote tallying. ICA at iii; *see also id.* at 3. Thomas Hicks, Chairman of the United States

¹⁰ See Taylor Hatmaker, “Exposed GOP Database Demonstrates the Risks of Data-Hungry Political Campaigns,” *TechCrunch* (June 19, 2017), available at <https://techcrunch.com/2017/06/19/deep-root-gop-data-leak-upguard/>.

Election Assistance Commission, testified before Congress last fall that hackers had breached Arizona and Illinois' voter registration lists.¹¹ More recently, the Department of Homeland Security reportedly notified officials in 21 states that their states' electoral systems were targeted by Russian hackers during the 2016 election.¹² Notably, Mr. Hicks observed in his testimony that a key strength of our electoral system is its decentralization, because "there is no national system that a hacker or bad actor can infiltrate to affect the American elections as a whole."¹³ A centralized voter registration database creates just such a target.

A number of current and former government officials have further warned that Russia and other foreign adversaries will seek to interfere in future elections and that such behavior may even escalate. Admiral Michael Rogers, director of the National Security Agency, testified before Congress that "[w]e have seen states seeking to shape the policies and attitudes of democratic peoples, and we are convinced such behavior will continue for as long as autocratic regimes believe they have more to gain than to lose by challenging their opponents in cyberspace."¹⁴ James Clapper, the former Director of National Intelligence, similarly testified that Russia is now "emboldened to continue" its election interference activities, "and to do so

¹¹ See Transcript, "Cybersecurity: Ensuring the Integrity of the Ballot Box," Hrg. before the House Comm. on Oversight and Gov't Reform, Subcomm. on Information Technology (Sept. 26, 2016), Statement of Thomas Hicks ("Hicks Statement"), at 17, available at <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg26124/pdf/CHRG-114hhrg26124.pdf>.

¹² Sari Horowitz et al., "DHS Tells States About Russian Hacking During 2016 Election," *Wash. Post* (Sept. 22, 2017), available at https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.56fba78532a2.

¹³ Hicks Statement at 12.

¹⁴ Statement of Adm. Michael S. Rogers, Commander, United States Cyber Command, before the Senate Comm. on Armed Services, at 2 (May 9, 2017), available at https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

even more intensely.”¹⁵ Members of Congress, meanwhile, have repeatedly expressed concerns about future election interference and the adequacy of existing measures to protect against further attacks, including potential tampering with voter registration systems.¹⁶

Finally, hostile nation-states could attempt to breach the Commission’s database for espionage purposes not directly related to election interference. For example, the Justice Department has charged two officers belonging to the Russian Federal Security Service (as well as two other individuals) with orchestrating a massive breach of Yahoo’s networks and accessing information regarding more than 500 million Yahoo user accounts.¹⁷ The indictment alleges that the conspirators used this information to target particular victims of interest to Russian intelligence as well as to orchestrate various scams.¹⁸ It has also been reported that other hacked files pertaining to American citizens are being used by foreign intelligence services, including in China and Russia, to assemble and cross-index databases that could be used to identify and even blackmail U.S. intelligence operatives.¹⁹

¹⁵ Statement of James R. Clapper before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism, at 5 (May 8, 2017), available at <https://www.judiciary.senate.gov/imo/media/doc/05-08-17%20Clapper%20Testimony.pdf>.

¹⁶ See, e.g., Video Recording, Hrg. before the Senate Comm. on Homeland Security and Governmental Affairs (Sept. 27, 2017) at 01:41:45 – 01:42:33 (questions from Sen. Claire McCaskill to Elaine Duke, Acting Secretary of DHS, and Christopher Wray, Director of the FBI, concerning measures to prevent interference in future elections); *id.* at 01:49:55 – 01:50:22 (question from Sen. James Lankford expressing concerns about tampering with voter registration lists), available at <https://www.c-span.org/video/?434411-1/senior-officials-testify-homeland-security-threats&start=6178>.

¹⁷ See Indictment, *United States v. Dokuchaev*, No. 3:17-cr-103, ECF No. 1 (N.D. Cal. Feb. 28, 2017).

¹⁸ *Id.* ¶¶ 34-39.

¹⁹ See Brian Bennet & W.J. Hennigan, “China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say,” *Los Angeles Times* (Aug. 31, 2015), <http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html>.

3. *The Commission's database could also be targeted by criminal actors seeking to sell personal data for profit*

Aggregating large volumes of PII also creates a target for malicious actors seeking to sell such information for profit. This information is valuable to cybercriminals because it can be used to commit identity theft and other acts of fraud. Indeed, there is a sophisticated global black market for stolen PII that reflects the value of this information.²⁰ The demand for stolen PII, in turn, fuels incentives for malicious actors to target networks with large data sets.

This reality has led courts to recognize that individuals whose personal data is stolen are at risk of identity theft. *See Attias v. CareFirst, Inc.*, 865 F.3d 620, 627-29 (D.C. Cir. 2017) (finding that plaintiffs established a “substantial risk” of identity theft after hackers breached the network of a healthcare provider and stole various types of PII); *Remijas v. Nieman Marcus Group, LLC*, 794 F.3d 688, 692-94 (7th Cir. 2015) (noting a similar risk and suggesting that, “[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities”). While credit card information may be in greater demand by some actors than the types of PII at issue here, malicious actors can use other types of information—particularly including names, addresses, and social security numbers—to sell for profit or to combine and cross-reference with other datasets to assemble more complete profiles of individuals targeted for identity theft.

There is also a distinct possibility that “ordinary” criminals who breach networks in order to obtain and sell PII could sell that information to parties with more hostile and dangerous ends

²⁰ *See, e.g.*, Lillian Ablon et al., *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation (2014), available at https://www.rand.org/pubs/research_reports/RR610.html; Jaikumar Vijayan, “The Identity Underworld: How Criminals Sell Your Data on the Dark Web,” *Christian Science Monitor* (May 6, 2015), available at <https://www.csmonitor.com/World/Passcode/2015/0506/The-identity-underworld-How-criminals-sell-your-data-on-the-Dark-Web>.

in mind. Last year, for example, Ardit Ferizi, a hacker who obtained PII about hundreds of U.S. citizens and provided this information to ISIS, pleaded guilty to hacking and providing material support for terrorism. *See* Statement of Facts, *United States v. Ferizi*, No. 1:16-cr-42, ECF No. 36 (E.D. Va. June 15, 2016) (describing facts admitted by Ferizi as part of a plea agreement). Ferizi admitted that he gained access to the server of a retail company based in the United States that contained the PII of tens of thousands of customers and culled that information to identify government employees and military service members. *Id.* at 3. He then passed that information to a well-known member of ISIS who posted it online and used it to call for attacks against specific individuals. *Id.* at 3-5.²¹

In this case, cyber criminals could conclude that a successful breach of the Commission's database would be rewarded by a substantial bounty from whatever buyer is most interested in obtaining and/or altering the information, and could seek to sell to the highest bidder this information or the tools that could be used to penetrate the database.

B. Storing Sensitive Personal Data on White House Systems Introduces Heightened Vulnerabilities

Federal networks are regularly targeted for attacks by malicious actors, including by nation-states and other sophisticated adversaries seeking precisely the type of information that the Commission is aggregating. As former Secretary of Homeland Security Michael Chertoff has warned in reference to the activities of the Commission:

We know that a database of personal information from all voting Americans would be attractive not only to adversaries seeking to affect voting but to criminals who could use the identifying information as a wedge into identity theft. We also know that foreign intelligence agencies seek large databases on Americans for intelligence and counterintelligence purposes. That is why the theft of more than 20 million personnel

²¹ Ferizi appears to have provided the information to ISIS free of charge. But other criminal actors could just as easily sell this type of information to a terrorist organization or hostile nation-state.

files from the U.S. Office of Personnel Management and the hacking of more than half a billion Yahoo accounts were such troubling incidents.²²

The Office of Personnel Management breach to which Secretary Chertoff referred was reported in 2015 and resulted in the exposure of the personal information of more than 20 million Americans. The Government Accountability Office (“GAO”) has repeatedly observed that breaches of federal networks are on the rise and that these attacks are evolving and becoming more sophisticated. *See, e.g.*, GAO, “Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System” (Jan. 2016) (noting that “[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive”).²³

Similarly, the White House has reported that federal agencies experienced 30,899 “reportable” cyber incidents for the 2016 fiscal year, 16 of which rose to the threshold of a “major incident” (meaning the incident involved certain types of critical information or that records were compromised on a large scale).²⁴ An Executive Order signed earlier this year took

²² Michael Chertoff, “Trump’s Voter Data Request Poses An Unnoticed Danger,” *Wash. Post* (July 15, 2017), available at https://www.washingtonpost.com/opinions/trumps-voter-data-request-poses-an-unnoticed-danger--to-national-security/2017/07/05/470efce0-60c9-11e7-8adc-fea80e32bf47_story.html?tid=a_inl&utm_term=.c07d23da07ef.

²³ Available at <https://www.gao.gov/assets/680/674829.pdf>. *See also* GAO, “Cybersecurity: Actions Needed to Strengthen U.S. Capabilities” (Feb. 2017), available at <https://www.gao.gov/assets/690/682756.pdf>

²⁴ *See* “Federal Information Security Modernization Act of 2014: Annual Report to Congress for Fiscal Year 2016,” at 111, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf.

note of these risks, highlighting among other findings that “[t]he executive branch has for too long accepted antiquated and difficult-to-defend [information technology].”²⁵

The Commission’s seemingly last-minute decision to move the database from the control of the Department of Defense (“DOD”) to the White House only exacerbates the database’s vulnerability. The Commission initially intended to use DOD’s Safe Access File Exchange (“SAFE”), which Vice Chair Kobach described in another lawsuit as a “tested and reliable method to secure file transfer used routinely by the military for large, unclassified data sets.” Decl. of Kris W. Kobach ¶ 5, *Elec. Privacy Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity* (“EPIC”), EFC No. 8, No. 1:17-cv-1320 (D.D.C. July 5, 2017). Just five days later, after the plaintiffs in that case amended their complaint to name DOD as a defendant, *see* ECF No. 21, *EPIC* (July 7, 2017), Vice Chair Kobach issued a new declaration stating that the Commission no longer intended to use DOD’s SAFE system and would instead “repurpos[e]” a White House system to accept the voter data. Third Decl. of Kris W. Kobach ¶ 1, ECF No. 24-1, *EPIC* (July 10, 2017) (“Third Kobach Declaration”).²⁶ The only explanation offered for the move was a somewhat cryptic statement that it was intended “not to impact the ability of other customers to use the DOD [SAFE] site.” *Id.* The Commission has also not disclosed which White House system has been “repurposed” to accept the PII of millions of Americans or what measures are in place to protect that data adequately, underscoring the importance of further factfinding on these matters. Based on what is already known, however, there is substantial

²⁵ Exec. Order No. 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (May 11, 2017), available at <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.

²⁶ These declarations have also been filed as exhibits to the Government’s Motion to Dismiss in this case. *See* ECF No. 27, Exhs. B and C.

reason to believe that the Commission has gone about its work in ways that subject the data to significant vulnerabilities and indeed exacerbate those vulnerabilities.

As an initial matter, this White House system has been newly developed—apparently within a matter of days. *See* Third Kobach Declaration ¶ 1 (stating that the new White House system was expected to be operational by later that day). As such, this new platform is effectively being tested for the first time through the ingestion of millions of data points about American voters. Additionally, the White House’s Information Technology staff does not have the same technical resources at its disposal to maintain large-scale databases as the Department of Defense.²⁷ Indeed, the Government has expressly affirmed that other White House components, such as the Executive Committee for Information Technology and the U.S. Digital Service, will have “no role” in administering the Commission’s database and that only a “limited number of [] technical staff” will be involved. Mot. to Dismiss, Exh. E, Decl. of Charles Christopher Herndon ¶ 6, ECF No. 27 (“Herndon Declaration”).

These limitations may well have been put in place in an effort to reduce the number of government officials with access to the information. But from a cybersecurity standpoint, the limited extent of information technology resources and personnel available to support the Commission’s work is alarming insofar as White House systems and personnel are regularly the subject of cyberattacks from sophisticated adversaries that require resource-intensive

²⁷ *See, e.g.*, Michael Shear, “Technology Upgrades Get White House Out of the 20th Century,” *N.Y. Times* (Apr. 3, 2016) (noting that “[u]ntil very recently, West Wing aides were stuck in a sad and stunning state of technological inferiority” and describing ongoing challenges), available at <https://www.nytimes.com/2016/04/04/us/politics/technology-upgrades-get-white-house-out-of-the-20th-century.html>.

responses.²⁸ Moreover, there is no indication that the Commission has taken the appropriate additional measures, and allocated the necessary additional resources, to fortify its database against these risks. Given that attempted attacks against White House unclassified networks are regularly reported in the media (and therefore should be well known to the Commission), this suggests an overall lack of attentiveness to the magnitude and gravity of the cybersecurity risks posed.²⁹

Mr. Herndon's Declaration describes certain basic measures that he avows have been taken or will be taken to secure the Commission's database, such as his assertion that the data will be encrypted and that Commission members will be able to access it through dedicated laptops with secure connection mechanisms. Herndon Declaration ¶ 5. But, on numerous other fronts, Mr. Herndon's Declaration is silent, leaving open the very real possibility that serious vulnerabilities remain in the way that the Commission is going about its work. Most notably, there is no indication that there are measures in place—including steps consistent with previous DHS recommendations for securing voter databases—that would: (1) restrict access only to Commission members as opposed to their staffs, or perhaps only those staff members specifically involved in analyzing the raw data; (2) restrict administrative privileges; (3) conduct

²⁸Jennifer Martinez, "White House Thwarts Hacker Attack on Unidentified Computer System," *The Hill* (Oct. 1, 2012), available at <http://thehill.com/policy/technology/259461-hackers-attack-white-house-computer-system>; Demetri Sevastopvlo, "Chinese Hack Into White House Network," *Financial Times* (Nov. 6, 2008), available at <https://www.ft.com/content/2931c542-ac35-11dd-bf71-000077b07658> (subscription required). See also Devlin Barrett & Siobhan Gorman, "Gmail Hack Targeted White House," *Wall St. J.* (June 3, 2011) (describing how Chinese hackers breached Gmail systems and targeted White House employees), available at <https://www.wsj.com/articles/SB10001424052702304563104576361863723857124> (subscription required).

²⁹See, e.g., Ellen Nakashima, "Hackers Breach Some White House Computers," *Wash. Post* (Oct. 28, 2014), available at https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html?utm_term=.7888768cd42e.

penetration testing and security audits; and (4) provide basic cybersecurity training to Commission members and their staffs, including training to avoid phishing attempts.³⁰ The need for basic cybersecurity training appears especially heightened in light of reports that a voter database previously created by Vice Chair Kobach is riddled with vulnerabilities, including through human errors such as officials sending passwords through email and even exposing them publicly.³¹ Finally, because no assurance has been given that the Commission's database would be wholly cut off from other White House systems, a breach of those other systems could provide a platform from which intruders could penetrate the database.

II. THE COMMISSION'S CREATION OF THIS DATABASE RUNS CONTRARY TO THE PURPOSES OF THE PRIVACY ACT AND COULD CAUSE SIGNIFICANT ONGOING HARM

A. The Commission's Conduct Runs Counter To The Privacy Act's Purpose Of Ensuring That Personal Data Handled By The Federal Government Receives Appropriate Protections

The Privacy Act expressly recognizes that the Government's ability to protect individual privacy is intertwined with its ability to provide security for personal information that it retains. The Privacy Act contains an extensive set of record-keeping requirements for covered records. Government agencies must maintain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency." 5 U.S.C. § 552a(e)(1). They must establish certain "rules of conduct" for personnel who have a role in administering records

³⁰ See United States Computer Emergency Readiness Team, "Securing Voter Registration Data" (last revised Sept. 30, 2016), available at <https://www.us-cert.gov/ncas/tips/ST16-001>.

³¹ See Dell Cameron, "Even a Novice Hacker Could Breach Network Hosting Kris Kobach's Bogus Voter Fraud Program," *Gizmodo.com* (Nov. 9, 2017), available at <https://gizmodo.com/even-a-novice-hacker-could-breach-the-network-hosting-k-1820263699>; Jessica Huseman & Derek Willis, "The Voter Fraud Commission Wants Your Data—But Experts Say They Can't Keep It Safe," *ProPublica* (Oct. 23, 2017), available at <https://www.propublica.org/article/crosscheck-the-voter-fraud-commission-wants-your-data-keep-it-safe>.

systems. *Id.* § 552a(e)(9). And, critically, agencies charged with handling covered records must establish “appropriate . . . safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.” *Id.* § 552a(e)(10).

When Congress enacted the statute in 1974, it was acutely aware that technological advances, including the ability to maintain large volumes of personal data on computer systems, posed new challenges for securing personal information retained by the Government. A study by the National Academy of Sciences that substantially informed the legislative process listed among the major priorities for public action the need to “increase[] work by the computer industry and professionals on security measures to make it possible for organizations to keep their promises of confidentiality.” S. Rep. No. 93-1183, at 6 (1974). Congress specifically sought to ensure “that certain computer hardware and software used to operate the information systems of government should provide features which will promote the necessary security of” those systems. *Id.* at 16. Although the Privacy Act does not mandate any specific set of technical standards, the Senate Committee Report explained that the term “adequate . . . standards” was meant to incorporate “safeguards which represent current state-of-the-art procedures at any given time.” *Id.* at 54; *see also id.* at 55 (noting that computer experts gave testimony about concerns such as “tapped transmissions” and that the National Academy of Sciences predicted that “the payoff in sensitive personal information to be obtained by . . . outsiders breaching system security is going to increase in the coming years”).

The facts in this case raise grave concerns that precisely mirror those considered by Congress in 1974. The Commission is aggregating a large-scale database that includes (or is

intended to include) voters' names, addresses, dates of birth, partial social security numbers, voting history, criminal records, and military status. *See supra* p. 5. That data is being ingested into a system designed by and accessible to Commission members as well as at least some White House personnel. *See* Herndon Declaration ¶¶ 3, 6. As already described, this aggregated information would be an extraordinarily valuable target for hackers—including hackers acting on behalf of foreign intelligence services as well as those operating for profit. Yet, apart from providing a months-old and generally vague declaration from another case describing how the database was *anticipated* to operate, the Government has provided no meaningful assurances about the measures that it is now using to secure this pool of data. *See* Herndon Declaration n.1 (noting that the declaration was originally filed on July 17, 2017 in a prior case).

Indeed, it is not even clear from the materials provided by the Government whether any specific person or entity is accountable for the security of the database. Mr. Herndon, who serves as the Director of White House Information Technology, stated that he was asked to “assist” in creating a mechanism to store this data on White House computer systems and that members of his technical staff would “assist” in the data collection process. Herndon Declaration ¶¶ 3, 6. Mr. Herndon also stated that White House network monitoring tools would log access to the database. *Id.* ¶ 6. Yet—in sharp contrast to the requirements of the Privacy Act—the Commission does not appear to have established any rules or procedures governing access to the database or any rules governing ongoing safeguards. *Cf., e.g., Doe v. Dep’t of Justice*, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) (noting that the Department of Justice has “promulgated extensive regulations . . . that safeguard its Privacy Act-protected records”) (internal quotations omitted); Memorandum from Jonathan R. Cantor, “DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information”

(Apr. 27, 2017) (providing guidance with respect to the handling of PII in the Department of Homeland Security, including information security requirements and restrictions on disseminating such information outside the Department).³² The Commission's operations thus stand at odds with the Privacy Act's clear purpose of ensuring that federal databases containing records about individuals maintain certain minimum safeguards to protect the security of those records.

B. The Commission's Aggregation Of This Data Could Cause Ongoing Harms That Would Be Difficult To Remedy

Due to the nature of data breaches, the Commission's aggregation of voter information could cause ongoing harms that would be difficult to remedy after they have occurred. Some states have already complied (or partially complied) with the Commission's requests, *see supra* p. 5, and others have indicated their intent to do so.³³ Whatever the extent of this compliance, the potential for harm can only increase so long as the database remains on White House systems and continues to grow. Voter data can become vulnerable to attack as soon as it is placed on White House systems. Once a network has been penetrated, hostile actors can begin exfiltrating data, often without the network administrator even becoming aware of the incident. In the case of the breach against OPM, for example, the intrusions were detected only after OPM installed new security systems, long after huge quantities of sensitive personal information had been stolen.³⁴ If the voter data at issue here is copied, it can never be fully erased or returned from the

³² Available at https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf

³³ *See* Associated Press, "How States Are Handling Trump's Voter Information Request," (Aug. 2, 2017) (cataloguing states' responses), available at <https://elections.ap.org/content/how-states-are-handling-trumps-voter-information-request>.

³⁴ *See* transcript, "OPM: Data Breach," Hrg. before the House Comm. on Oversight and Gov't Reform, at 42-43 (June 16, 2015), available at <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99659/pdf/CHRG-114hhrg99659.pdf>.

possession of those who gain improper access to it. Moreover, if it is altered, that alteration could be difficult to detect and could cause widespread confusion for months or years to come.

CONCLUSION

The Court should deny the Government's motion to dismiss. In the alternative, the Court should grant Plaintiffs' request to conduct jurisdictional discovery.

Respectfully submitted,

/s/ _____
JOSHUA A. GELTZER (D.C. Bar No. 1018768)
INSTITUTE FOR CONSTITUTIONAL
ADVOCACY AND PROTECTION
Georgetown University Law Center
600 New Jersey Ave., N.W.
Washington, D.C. 20001
Telephone: 202.661.6728
JG1861@Georgetown.edu

ROBERT S. LITT*
DAVID A. NEWMAN*
SOPHIA M. BRILL*
MORRISON & FOERSTER LLP
2000 Pennsylvania Ave., N.W.
Washington, D.C. 20006

ROBERT TAJ MOORE*
MORRISON & FOERSTER LLP
250 West 55th Street
New York, N.Y. 10019

Counsel for Amici Curiae

* *pro hac vice* motions pending

APPENDIX: LIST OF AMICI CURIAE

1. James R. Clapper served as the U.S. Director of National Intelligence (DNI) from 2010 to January 20, 2017. Prior to becoming the DNI, he served for over three years in two administrations as the Under Secretary of Defense for Intelligence, where he was dual-hatted as the Director of Defense Intelligence for the DNI and as the Director of the National Geospatial-Intelligence Agency from 2001 to 2006.

2. Dipayan Ghosh served as Senior Advisor on Technology Policy at the Office of Science and Technology Policy and National Economic Council in the White House from 2013 to 2015, and until recently served as a privacy and public policy advisor at Facebook.

3. Andrew J. Grotto served as the Senior Director for Cybersecurity Policy at the White House from 2016 to 2017. He previously served as Senior Advisor for Technology Policy at the Department of Commerce.

4. Nancy Libin served as Chief Privacy Officer at the U.S. Department of Justice from 2009 to 2012.

5. Alex Macgillivray was Deputy United States Chief Technology Officer from 2014 to 2017. He previously served as General Counsel at Twitter and Deputy General Counsel at Google.

6. Matthew G. Olsen served as Director of the National Counterterrorism Center from 2011 to 2014. He previously served as the General Counsel for the National Security Agency and in various national security-related roles at the Department of Justice.

7. Christopher Painter served as the Coordinator for Cyber Issues at the Department of State from 2011 to 2017.

8. Paul Rosenzweig is a Senior Fellow at the R Street Institute. He teaches Cybersecurity Law and Policy at George Washington University School of Law. He served as Deputy Assistant Secretary for Policy at the Department of Homeland Security from 2006 to 2009.

9. Suzanne Spaulding served from 2011 to 2017 as the Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security, which is charged with strengthening cybersecurity and protecting the nation's critical infrastructure.

CERTIFICATE OF SERVICE

I hereby certify that on December 5, 2017, I filed this Motion with the United States District Court for the District of Columbia using the CM/ECF system, which will cause it to be served on all counsel of record.

Dated: December 5, 2017

Respectfully submitted,

/S/

JOSHUA A. GELTZER (D.C. Bar No. 1018768)
INSTITUTE FOR CONSTITUTIONAL
ADVOCACY AND PROTECTION
Georgetown University Law Center
600 New Jersey Ave. NW
Washington D.C. 20001
Telephone: 202.661.6728
JG1861@Georgetown.edu