



A. A temporary restraining order in favor of Plaintiffs and against the Defendants, and entry of a temporary injunction enjoining the Defendants, Secretary of State Rolando Pablos, and Keith Ingram, Director, Texas Elections Division, from providing the Voter List and any part thereof to the Commission, and to take all actions necessary to maintain the status quo ante pending a determination on the merits; and

B. Such other and further relief as the Court deems just in the premises.

Respectfully submitted,

LAW OFFICE OF CHARLES McGARRY

/s/ Charles W. McGarry

Charles W. McGarry

Texas Bar No. 13610650

701 Commerce Street, Suite 400

Dallas, Texas 75202

(214) 748-0800

(214) 748-9449 fax

[cmcgarry@ix.netcom.com](mailto:cmcgarry@ix.netcom.com)

Myrna Pérez, Esq.

Tomas Lopez, Esq.

**Brennan Center for Justice**

120 Broadway, Suite 1750

New York, NY 10271

(646) 292-8310 phone

(212) 463-7308 fax

[myrna.perez@nyu.edu](mailto:myrna.perez@nyu.edu)

[wendy.weiser@nyu.edu](mailto:wendy.weiser@nyu.edu)

[tomas.lopez@nyu.edu](mailto:tomas.lopez@nyu.edu)

*(Applications for admission*

*pro hac vice forthcoming)*

Daniel T. Donovan, Esq.  
Susan M. Davies, Esq.  
Michael A. Glick, Esq.  
**Kirkland & Ellis LLP**  
655 Fifteenth Street, N.W.  
Washington, DC 20005  
(202) 879-5000 phone  
(202) 879-5200 fax  
[daniel.donovan@kirkland.com](mailto:daniel.donovan@kirkland.com)  
[susan.davies@kirkland.com](mailto:susan.davies@kirkland.com)  
[michael.glick@kirkland.com](mailto:michael.glick@kirkland.com)  
*(Applications for admission pro hac vice  
forthcoming)*

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

This is to certify that a true and correct copy of this instrument was delivered to the following attorney of record on this 29<sup>th</sup> day of September, 2017, in accordance with the Texas Rules of Civil Procedure:

Esteban S.M. Soto  
Assistant Attorney General  
General Litigation Division  
Office of the Attorney General  
300 West 15th Street  
Austin, TX 78701  
Phone: 512-475-4054  
Fax: 512-320-0667  
[Esteban.Soto@oag.texas.gov](mailto:Esteban.Soto@oag.texas.gov)

/s/ Charles W. McGarry  
Charles W. McGarry



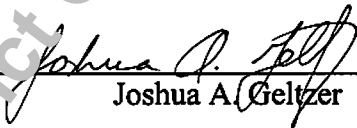
requiring from the Commission any commitments for keeping that data secure would leave Texas voters' private information particularly appealing and vulnerable to hackers, including those acting in association with foreign powers. This is so for at least three reasons.

5. First, voter data has been, and continues to be, a particular target for hackers, meaning that the sharing of such data inherently raises cybersecurity risks not necessarily associated with other information. This is a consensus view among those in the field of cybersecurity and national security. For example, former Secretary of Homeland Security Michael Chertoff recently articulated this widely held assessment. A true and correct copy of Secretary Chertoff's column, downloaded from the *Washington Post* website, is attached hereto as Exhibit B.
6. Second, the holdings of Federal Government entities can represent a particularly attractive target for hacking because hackers previously have demonstrated such entities' security measures to be inadequate. I know this based on my experience working on cybersecurity matters in the Federal Government as well as based on public reporting of incidents, including the Federal Government's own public pronouncements, such as its acknowledgement in June 2015 that the Office of Personnel Management (OPM) had been successfully targeted in a data breach affecting the records of millions of individuals. In the absence of public commitments by the Commission to protect data provided to it, hackers will see the transfer of data to the Commission as an invitation to continue to exploit weaknesses.
7. Third, the vastness of the Commission's request and the Commission's apparent intent to aggregate the data provided in response to it—that is, the effort to acquire a huge amount of sensitive data and hold it in a single, high-profile place—increases cyber threats to the data. The Commission is attempting to collect data from every state in the nation and then centralize the data in a single repository managed by the Executive Office of the President. This centralization of data increases the appeal—and therefore the risk—of hacking by reducing the burden on hackers who seek to penetrate voter data systems. This is true even if some or all the same information could, at least in theory, be acquired in some other manner or from some other source(s), because amassing all of it in a single, high-profile, purportedly authoritative place materially heightens the appeal and payoff associated with hacking that one storage location.
8. Defendants could and should demand that the Commission undertake certain basic steps in order to protect Texas voters' data if it is to be shared with the Commission. Those steps include encryption of the data while in transit and in storage; the requirement of multi-factor authentication to access the data; restriction of access to a clearly defined and minimally necessary list of authorized individuals with separate user accounts; credible and independent audits of the database; and air-gapping of the database. A true and correct copy of a recent column in which two coauthors and I outline these five steps, downloaded from the *Hill* website, is attached hereto as Exhibit C.

9. In my opinion, if Defendants do not require the Commission to institute adequate protective measures, release of the data to the Commission will immediately invite privacy and security violations for Texans' whose data is shared. If the security of that data is compromised, the injuries that could befall Texans range from unwanted commercial solicitation, to personalized harassment, to identity theft, to attempt by foreign powers to meddle in the administration of elections held in the United States.
10. I would do my best to make myself available to the Court and the parties in the case to elaborate on the opinions stated herein.

My name is Joshua A. Geltzer; my date of birth is February 7, 1983; my office address is 600 New Jersey Avenue NW, Washington, D.C., 20001; and I declare under penalty of perjury that the foregoing is true and correct.

Executed in Washington, D.C., on the 28<sup>th</sup> day of September, 2017.

  
\_\_\_\_\_  
Joshua A. Geltzer

# EXHIBIT A

Unofficial copy Travis Co. District Clerk Velva L. Price

**JOSHUA A. GELTZER**

2823 Q Street NW Washington, DC 20007 (917) 992-2600 JGeltzer@gmail.com

**SELECTED EXPERIENCE**

**EXECUTIVE DIRECTOR AND VISITING PROFESSOR OF LAW, INSTITUTE FOR CONSTITUTIONAL ADVOCACY AND PROTECTION, GEORGETOWN UNIVERSITY LAW CENTER** 2017-present  
Building new institute to promote constitutional values through impact litigation, public education, and scholarship.

**SENIOR DIRECTOR FOR COUNTERTERRORISM, NATIONAL SECURITY COUNCIL** 2015-2017  
Coordinated development of U.S. counterterrorism policy and advised White House leadership on terrorist threats.

**DEPUTY LEGAL ADVISER TO THE NATIONAL SECURITY COUNCIL** February-October 2015  
Counseled NSC leadership on legal issues regarding counterterrorism, intelligence collection and cyber matters.

**COUNSEL TO THE ASS'T ATTORNEY GENERAL FOR NAT'L SECURITY, DEPARTMENT OF JUSTICE** 2013-2015  
Advised DOJ leadership on global counterterrorism issues, FISA matters, and national security-related litigation.

**LAW CLERK TO JUSTICE STEPHEN BREYER, U.S. SUPREME COURT** 2012-2013  
Analyzed petitions for certiorari; prepared the Justice for oral argument; and drafted opinions and memorandums.

**LAW CLERK TO CHIEF JUDGE ALEX KOZINSKI, NINTH CIRCUIT COURT OF APPEALS** 2011-2012  
Wrote bench memos to prepare the Judge for oral arguments and assisted him with drafting opinions and orders.

**EDUCATION**

**YALE LAW SCHOOL**, New Haven, CT

J.D., May 2011; Olin Fellow, Yale Law School Center for Studies in Law, Economics, & Public Policy

*Activities:* *Yale Law Journal*, Editor-in-Chief; research assistant to Professors Akhil Amar and Amy Chua

*Experience:* Summer Law Clerk, Office of the Legal Adviser, Department of State

Summer Associate, Covington & Burling LLP

Summer Law Clerk, Counterterrorism Section, Department of Justice

**KING'S COLLEGE LONDON**, London, UK (Marshill Scholarship)

Ph.D., War Studies, 2008; M.A., International Relations, 2006 (awarded with distinction)

*Dissertation:* *Al-Qaeda as Audience: Signalling in U.S. Counter-terrorist Policy & the al-Qaeda World-view*

*Activities:* King's Postgraduate Conference, Chair; European Foreign Policy Conference, Editorial Director

**PRINCETON UNIVERSITY**, Princeton, NJ

A.B., Woodrow Wilson School of Public and International Affairs, 2005. GPA: 3.97

*Honors:* *Summa cum Laude*; Phi Beta Kappa; Senior with the Highest Academic Standing Award

**SELECTED PUBLICATIONS**

- "Of Suspension, Due Process, and Guantanamo," *Journal of Constitutional Law*, Vol. 14, No. 3 (2012).
- "Reconstructing the Republic: The Great Transition of the 1860s," with Amar & Worth, in *Transitions: Legal Change, Legal Meanings*, Austin Sarat, ed. (University of Alabama Press: 2012).
- "Asymmetric Strategies as Strategies of the Strong," with Breen, *Parameters*, Vol. 41, No. 1 (2011).
- "Taking Hand-Offs or Going It Alone," *Studies in Conflict & Terrorism*, Vol. 34, No. 2 (2011).
- "Decisions Detained: The Courts' Embrace of Complexity in Guantánamo-Related Litigation," *Berkeley Journal of International Law*, Vol. 29, No. 1 (2010).
- *U.S. Counter-Terrorism Strategy & al-Qaeda: Signalling & the Terrorist World-View* (Routledge: 2009).
- "The Non-Kinetic Aspects of Kinetic Efforts," in *Influence Warfare: How Terrorists & Governments Fight to Shape Perceptions in a War of Ideas*, James Forest, ed. (Praeger Security International: 2009).

**MEMBERSHIPS**

- Term Member, Council on Foreign Relations
- Fellow, American Bar Foundation
- Advisory Committee Member, American Bar Association Standing Committee on Law and National Security

**SKILLS AND INTERESTS**

Play rock guitar and classical violin. Enjoy baseball, hockey, literature, new restaurants, and travel.



# EXHIBIT B

Unofficial copy Travis Co. District Clerk Velva L. Price

# Trump's voter data request poses an unnoticed danger

By Michael Chertoff July 5

*Michael Chertoff, U.S. homeland security secretary from 2005 to 2009, is executive chairman of the Chertoff Group, a security and risk-management advisory firm.*

The Trump administration's Presidential Advisory Commission on Election Integrity is asking states for voter-registration data from as far back as 2006. This would include names, dates of birth, voting histories, party registrations and the last four digits of voters' Social Security numbers. The request has engendered controversy, to put it mildly, including refusals by many states and a caustic presidential tweet.

But whatever the political, legal and constitutional issues raised by this data request, one issue has barely been part of the public discussion: national security. If this sensitive data is to be collected and aggregated by the federal government, then the administration should honor its own recent cybersecurity executive order and ensure that the data is not stolen by hackers or insiders.

We know that voting information has been the target of hackers. News reports indicate that election-related systems in as many as 39 states were penetrated, focusing on campaign finance, registration and even personal data of the type being sought by the election integrity commission. Ironically, although many of these individual databases are vulnerable, there is some protection in the fact that U.S. voting systems are distributed among thousands of jurisdictions. As data-security experts will tell you, widespread distribution of individual data elements in multiple separate repositories is one way to reduce the vulnerability of the overall database.

That's why the commission's call to assemble all this voter data in federal hands raises the question: What is the plan to protect it? 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 files from the U.S. Office of Personnel Management and the hacking of more than half a billion Yahoo accounts were such troubling incidents.

Congress and the states need to be advised on how any data would be housed and where. Would it be encrypted? Who would have administrative access to the data, and what restrictions would be placed on its use? Would those granted access be

subject to security background investigations, and would their behavior be supervised to prevent the kind of insider theft that we saw with Edward Snowden or others who have released or sold sensitive data? What kinds of audit procedures would be in place? Finally, can the security risk of assembling so much tempting data in one place be mitigated by reducing and anonymizing the individual voter information being sought?

In May, President Trump signed the executive order on cybersecurity to instill tough security in federal offices that handle critical government data. That order is a commendable initiative to hold officials accountable for safeguarding sensitive personal information, such as voter information. The president's election integrity commission should live up to the president's own directive.

**Read more on this issue:**

Michael Waldman: Commission on 'election integrity' could instead restrict voting

The Post's View: Trump launches his opening voter suppression salvo

The Post's View: Trump's commission on voter fraud is, well, fraudulent

Fareed Zakaria: America must defend itself against the real national security menace

Unofficial copy Travis Co. District Clerk Velda L Price

# EXHIBIT C

Unofficial copy Travis Co. District Clerk Velva L. Price



# Trump's voter fraud commission must protect data from hacker

BY RAJESH DE, JOSHUA GELTZER AND MATTHEW OLSEN, OPINION CONTRIBUTORS - 08/24/17 05:00 PM EDT

16 SHARES

SHARE

TWEET

PL

## Just In...

**Tech, Trump see rare consensus with GOP tax plan**

TECHNOLOGY — 16M 23S AGO

**Dem addiction to Trump attacks gives party cause for concern**

CAMPAIGN — 16M 27S AGO

**Anti-abortion groups fuming over GOP failure to defund Planned Parenthood**

HEALTHCARE — 16M 31S AGO

**Distrust of Senate grows within GOP**

SENATE — 16M 35S AGO

**Trump to rally manufacturers in tax speech Friday**

FINANCE — 18M 4S AGO

**Trump-Russia pundit mulling run for Illinois attorney general**

BLOG BRIEFING ROOM — 7H 8M AGO

**Stephen King on Trump's tax plan: Trump 'couldn't give a s---' about working class**

IN THE KNOW — 7H 8M AGO

**NBA commissioner's 'expectation' is that players stand for anthem**

BLOG BRIEFING ROOM — 7H 27M AGO



© Getty Images

Many states have responded with alarm to the massive data call issued by the Presidential Advisory Commission on Election Integrity co-chaired by Vice President Mike Pence and Kansas Secretary of State Kris Kobach. State election officials have voiced concerns that the commission's real agenda is to generate support for election laws that suppress voter participation. Indeed, 21 states and the District of Columbia declined to provide any data in response to the commission's initial outreach, which a federal district judge made clear is merely a request, not a lawful demand.

Perhaps most colorfully, Mississippi's secretary of state responded to the request by saying that the commission "can go jump in the Gulf of Mexico and Mississippi is a great State to launch from." The commission's request for Social Security numbers was refused by none other than Secretary of State Kobach himself on Kansas's behalf. Even as many states reaffirm their refusals to provide any information, others are providing a considerable amount of data on their voters. And this raises an additional and significant concern about the commission's work: the lack of protection for this sensitive data.

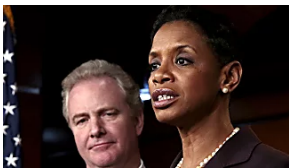
As former Homeland Security Secretary Michael Chertoff has rightly emphasized, the ingestion and aggregation of this massive amount of massively sensitive information poses its own form of threat. It provides a single, seductive target for the many actors we now know are keen to manipulate and undermine confidence in our elections, as well as to gather detailed information on Americans for espionage purposes.

[VIEW ALL](#)

Related News by



Drug Enforcement chief to step down: report



Dem calls for all NFL players to kneel during...



Ex-Obama adviser: 'God save us' if Kim Jong Un...



DeVos flies on her own private jet for...

So, as states consider what information to provide to the commission, they owe it to their voters and the sanctity of the elections our country's laws entrust them to administer to consider how that information should be handled once provided. Indeed, some state laws impose rules and requirements for accessing sensitive electoral data. Beyond that, and regardless of any state's particular laws, respect for America's voters and elections requires sensible protection of the data.

The Trump administration must take seriously the responsibility of safeguarding of the data its commission is requesting. Unfortunately, the administration deliberately moved the commission's "administrative home" from the U.S. Department of Defense, which had already designed a website to receive the data requested, to the Executive Office of the President, raising concerns that the move was designed to cloak the commission's work from transparency laws, since the Freedom of Information Act applies to virtually all departments and agencies across the federal government but not to the Executive Office of the President.

The Defense Department, of course, has at its disposal the resources and expertise of the National Security Agency and U.S. military in protecting the transmission of sensitive data, in stark contrast to the limited capacity of the White House Executive Office. That puts an even higher burden on the states to demand that the commission at least take certain basic cybersecurity steps if those states are to comply — voluntarily — with the commission's unprecedented data request. We urge at least five such steps.

First, the information should be encrypted, while in transit to and within the commission as well as when stored by it. Encrypted data, even if stolen, needs to be decrypted, an often insurmountable challenge even for governments. That's why encryption has become the norm for many email providers, messaging apps and hardware such as cell phones and laptops.

Second, multi-factor authentication should be required to access the data. This, too, is becoming common practice: If you don't already require your email provider to confirm that you're really you when logging in for the first time from a new computer or device, you're significantly risking the security of your email while sparing yourself ten seconds of minor inconvenience. The same should be required to access this sensitive data.

Third, access to the data should be restricted to a clearly defined minimally necessary list of authorized individuals with separate user accounts on a strict need-to-know basis. This minimizes the inherent vulnerability associated with every additional user and puts on notice every user that the circle of potential culprits is small if information leaks out. And, while passwords aren't a sufficient defense on their own, they should be complex and unique for authorized users.

Fourth, credible and independent cybersecurity audits of the commission's database should be conducted on a periodic basis, which in turns requires that the database be designed so that every access to it can be traced in order to facilitate such audits. Many cyber intrusions and exfiltrations occur for months or even years before they're noticed; but periodic audits can identify breaches and stop the bleeding far more quickly.

Fifth, the database should be "air-gapped," meaning it should be held on a segmented network not connected to the internet. This helps to insulate and thus protect the database. It also means that, when the commission's work is done, the data held there can and should be deleted with accompanying certification by the commission's co-chairs.

From a cybersecurity standpoint, it's simply a bad idea to put all of this sensitive information in one place. But if the administration is committed to gathering this data, then failing to take the steps outlined above is indefensible. In an era when the commission's database is a prime target for adversaries foreign and domestic keen to sabotage and distort our democratic system, protecting America's elections demands protecting American voters.

*Rajesh De served as general counsel of the [National Security Agency](#) during the Obama administration. He now leads the cybersecurity and data security practice and co-leads the national security practice at [Mayer Brown LLP](#), where he is a partner.*

*Joshua A. Geltzer served as senior director for counterterrorism and deputy legal advisor at the [National Security Council](#) during the Obama administration. He is now executive director and visiting professor of law at the [Institute for Constitutional Advocacy and Protection](#) at [Georgetown University](#).*

*Matthew G. Olsen served as director of the National Counterterrorism Center during the Obama administration. He is now an adjunct senior fellow at the [Center for a New American Security](#) and co-founder of technology firm [IronNet Cybersecurity](#).*

---

*The views expressed by contributors are their own and are not the views of The Hill.*

**TAGS** MIKE PENCE VOTER FRAUD DONALD TRUMP KRIS KOBACH MICHAEL CHERTOFF STATES ADMINISTRATION WHITE HOUSE GOVERNMENT TECHNOLOGY CYBERSECURITY

SHARE

TWEET

PLUS ONE



THE HILL 1625 K STREET, NW SUITE 900 WASHINGTON DC 20006 | 202-628-8500 TEL | 202-628-8503 FAX  
THE CONTENTS OF THIS SITE ARE ©2017 CAPITOL HILL PUBLISHING CORP., A SUBSIDIARY OF NEWS COMMUNICATIONS, INC.

Unofficial Copy Travis Co. District Clerk Nova L. Price