

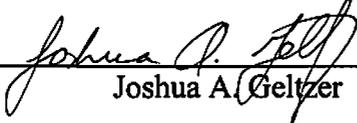
requiring from the Commission any commitments for keeping that data secure would leave Texas voters' private information particularly appealing and vulnerable to hackers, including those acting in association with foreign powers. This is so for at least three reasons.

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 attempts 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 28th day of September, 2017.



Joshua A. Geltzer