UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

Mathew Harley , et al., *Plaintiffs*, - against - Peter S. Kosinski, et al., *Defendants*.	Case No: 20-CV-4664 **DECLARATION OF ANDREW W. APPEL**

ANDREW W. APPEL, declares the following to be true and correct under penalty of perjury, pursuant to 28 U.S.C. § 1746:

1. I am a Professor of Computer Science and former Chair of the Department of Computer Science at Princeton University. I have been on the faculty of Princeton University for 34 years; my CV is attached to this declaration as Exhibit A. My research is in software verification, programming languages, computer security, and technology policy—particularly voting systems. I have served as an expert witness regarding the security of election equipment and voting systems in numerous court proceedings.

2. I submit this Declaration in opposition to the plaintiffs' motion for a preliminary injunction that would require election officials of seven states to "accept voted ballots from overseas voters that are sent via email or facsimile to the local election office (whether directly or through DoD Fax)."

3. It is a very well established scientific consensus that the Internet should not be used for the return of voted ballots in public elections. A 2018 Consensus Study Report of the National Academies of Sciences, Engineering, and Medicine (NASEM), attached as Exhibit B, stated, "At

the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet." (at page 9 and page 106)

4. This NASEM study committee was chaired by two university presidents and was comprised of five computer scientists, a mathematician, two social scientists, a law professor, and three state and local election administrators. I served on this committee, and I am confident that the report presents the clear consensus of the scientific community, as represented not only by the members of the committee but also the 14 external reviewers—election officials, computer scientists, experts on elections—who were part of the National Academies' process. This conclusion, which is also my own expert opinion regarding Internet voting, is backed up by numerous scientific papers.

5. A May 2020 report from CISA, the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security, attached as Exhibit C, lists the "Electronic transmission of voted ballot" as "High" risk, lists "Electronic ballot marking" as "Moderate" risk, and lists "Electronic ballot delivery (digital copies of blank ballots provided to voter)" as "Low" risk. These assessments are consistent with the scientific consensus, and with my own opinion. It is my expert opinion that, given the current technology, the security risks of returning voted absentee ballots by the internet or fax are so substantial that they significantly outweigh the burdens on overseas voters to return their ballots by the means that are currently available.

6. I have reviewed the declarations in support of plaintiffs' preliminary injunction motion. They seem to misunderstand the technology of fax transmissions. Once upon a time, a

"fax machine" was connected to a "land line" that went through the "phone network." How safe that was in 1985 is no longer relevant today, when nobody has a "fax machine" and the "phone network" is the Internet. Most voters, and many election administrators, use on-line fax services such as HelloFax. The voter logs in (via the Internet) and uploads a PDF file; the fax service converts it to a fax-format bitstream and sends it into the part of the Internet called "the phone system"; the receiver logs in (via the Internet, perhaps to a different on-line fax service) and downloads a PDF file that has been converted from the bitstream. This has so many points of insecurity: the sender's online-fax service company may be more or less vulnerable to hackers (or insiders); the receiver's online-fax service, ditto; and the fax-format bitstream is transmitted unencrypted, unauthenticated across the phone network.

7. Even if both the voter and the LEO had old-fashioned fax machines that they directly plugged into old-fashioned phone lines, the phone network is now a part of the Internet, and is hackable by hackers located on the Internet. I have written about that in this article: https://freedom-to-tinker.com/2018/02/22/are-voting-machine-modems-truly-divorced-from-the-internet/ , attached as Exhibit D. In summary, regarding fax: fax transmission is as insecure as other internet-based means of transmission, because (nowadays) fax *is* an internet-based means of transmission. That the receiving fax machine may be operated by the Federal Voter Assistance Project of the Department of Defense, sometimes described as "DoD fax," does not change my conclusion that the system of ballot transmission has high risk vulnerability to hacking.

8. Paragraph 28 of the Bryan Declaration (ECF #13-2), exhibits the confusion about the technology: "All 50 states are required by the MOVE Act to be able to transmit ballots to voters electronically, but voters can ask to receive their ballots by email/online or fax as well." But

email is clearly an electronic means of transmission, so is "online", and so is fax.

9. Paragraph 12 of the Burch Declaration (ECF #13-3) suffers from similar misunderstanding. "Email and facsimile voting are not the same thing as electronic voting; there is always a paper trail with casting a voted ballot by email or facsimile." But this is not true at all, in any meaningful way. The transmission of the ballot image from the voter's computer or fax machine to a local election official's computer or fax machine is purely electronic, and has no paper trail. The only paper is *local*, does not in any meaningful sense form a "trail" that could be used to assure that the candidates selected by the voter are the ones counted by the LEO. That is, if the voter prints out a ballot, marks votes on the paper, then puts the paper in a fax machine, there is one *segment* of a paper trail that begins and ends in the voter's apartment. Then if the local election official receives a ballot via fax, prints it on paper, and runs it through an optical-scan voting machine, there is a *segment* of a paper trail that begins and ends at the LEO's office. These two segments do not form a *trail*, because there is an enormous gap in the middle: electronic transmission through hackable computers and hackable networks. If instead of fax, the voter scans in the marked paper ballot and then e-mails it or uploads it to an internet server, then the same is true: this segment of a paper "trail" begins and ends in the voter's apartment, and there is a huge gap in the middle where an insecure electronic communication (from the voter's computer sending the e-mail or upload, to the LEO's computer receiving an e-mail or download) is subject to fraudulent alteration by hackers.

10. Internet voting—that is, the transmission of voted ballots from voters to election administrators in digital form over the internet—is known to be inherently insecure, as I have explained above. This is equally true if it is called something else, like "online voting" or "e-mail ballot return" or "fax." And when we examine *specific* internet voting systems from

specific private vendors that public officials have proposed for use in public elections, we find that these systems have even more security flaws than is already inherent in the use of the internet. If state election officials were compelled to adopt online ballot return, they would necessarily have to choose some specific system—to do a thing one must have a means to do it.

11. Regarding these specific online-ballot return systems, the recent scientific literature has several studies, in most cases peer reviewed, reporting on severe security and privacy flaws in these systems based on examinations by computer scientists. A system piloted for municipal elections in Washington DC was found by independent researchers[1] to have so many severe security flaws, that it was abandoned before being used in an election. A system sold by Scytl for use in Swiss elections was found by independent researchers[2] to have so many severe security flaws, that it was abandoned before being used in an election. A system sold by Voatz for use in West Virginia was found by independent researchers[3] to have so many severe security flaws, that the State abandoned its use. A system sold by Democracy Live for use in New Jersey elections was found by independent researchers[4] to have severe security and privacy flaws, and New Jersey soon after completely abandoned electronic ballot return[5].

---

[1] Attacking the Washington, D.C. Internet Voting System Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. A. Halderman. In Angelos D. Keromytis, editor, *Financial Cryptography and Data Security (FC)*, volume 7397 of Lecture Notes in Computer Science, pages 114–128. Springer, 2012.

[2] Ceci n'est pas une preuve: the use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system, by Sarah Jamie Lewis , Olivier Pereira, and Vanessa Teague, https://blog.fdik.org/2019-03/UniversalVerifiabilitySwissPost.pdf, March 2019.

[3] The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections, by Michael A. Specter, James Koppel, and Daniel Weitzner, in *29th USENIX Security Symposium*, February 2020.

[4] Security Analysis of the Democracy Live Online Voting System, by Michael A. Specter and J. Alex Halderman, https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf, June 2020.

[5] in part because of these specific flaws, and in part because New Jersey law prohibits connecting voting systems to the Internet.

12. So, in summary, electronic ballot return is inherently insecure—that is the clear scientific consensus—and any *particular* implementation of electronic ballot return tends to be even more insecure, in surprising and unpredictable ways—that is the empirical observation of study after study. The high risk of electronic ballot return is a good reason for these seven states to avoid this practice.

Dated: October 8, 2020
Princeton, New Jersey

Andrew W. Appel