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 DAVID JEFFERSON

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

1. I am a computer scientist at the Lawrence Livermore National Laboratory, which describes itself as a "premier research and development institution for science and technology applied to national security." Its principal responsibility is ensuring the safety, security and reliability of the nation's nuclear weapons through the application of advanced science, engineering, and technology. I thus have a background in national security issues. I am employed in the Center for Applied Scientific Computing supercomputing applications, specifically large scale parallel discrete event simulations. Before joining Lawrence Livermore National Laboratory I spent seven years in Silicon Valley at the DEC/Compaq/HP Labs doing Internet-related work, specializing in election security. Earlier, I was a professor of computer science at the University of Southern California (USC) and at UCLA, and I conducted research in the fields of parallel discrete event simulation, simulated evolution, parallel operating systems, and robotics. I am the coinventor of the Time Warp method of parallel discrete event simulation.

2. I am a member of the Board of Directors of Verified Voting, the best known and

oldest nonpartisan, nonprofit organization devoted entirely to the safety and security of our election technologies.

3. I am also a member of the Board of Directors of the California Voter Foundation, another nonpartisan, nonprofit organization devoted to mechanisms and procedures for the conduct of free and fair elections, and in helping create an informed citizenry about all election processes.

4. 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)." I submit this Declaration in my own capacity and not as a representative of Lawrence Livermore National Laboratory or any other organization.

5. As a computer scientist I have also studied election technology, election security and election cybersecurity for over 20 years. I was Chair of the Technical Committee of the California Secretary of State Bill Jones' Task Force on Internet Voting from 1999-2000. That task force conducted what was probably the first ever study on Internet voting under government auspices. To the surprise of many, including ourselves considering our initial expectations, our conclusion even then was that Internet voting was too dangerous to offer for public elections. There were too many fundamental ways in which such elections could be compromised. We considered all forms of Internet voting, including web-based and email-based, and essentially all of those vulnerabilities are still with us 20 years later.

6. Since 2000 I have participated in many studies of Internet voting as advisor to governments and in academic settings. I have written and spoken and testified extensively on the subject, and been sought out by media many times to address the vulnerabilities of online voting.

7. Over the years the terms "Internet voting" and "online voting" and "remote electronic voting", all of which mean essentially the same thing, have expanded beyond email- and web-based voting to include FAX voting and mobile app voting. Many of the vulnerabilities I will discuss apply to all of them. Some, however, are specific to email and FAX voting.

8. Voting security is a matter of U.S. national security. Obviously the legitimacy of democratic government depends upon the idea that elections are free and fair and that the outcome truly represents the will of the people, the "consent of the governed". The general problem with *all* forms of Internet voting is that it is not possible with any technologies today or any expected to be available in the foreseeable future, to guarantee the integrity of the election. Anyone in the world with an internet connection, whether an adversary nation state, a criminal syndicate, our own domestic partisans, or even a lone hacker sitting halfway around the world, can *disrupt an election* conducted over the Internet, *destroy ballots*, *change the contents of ballots*, *violate the secrecy of the ballots*, and *change the outcome of an election*.

9. An attacker can achieve his purpose, and do so, quite possibly undetected, so that no one — not voters, not election officials, and not even the "winner" who benefitted from the surreptitious cyberattack — would know that the outcome was changed. Even if an attack were somehow detected by officials, they would likely no know with any precision how many, or which, ballots were affected, so they would not be able correct the results or know for sure whether the winner was correctly called. Moreover, they would likely not be able to identify who conducted the attack, and even if they did, the attackers could very well be beyond the reach of U.S. law, as indeed the Russian agents who meddled with the 2016 election are.

10. Before identifying specific vulnerabilities in email and FAX voting, I will list some of the generic attacks that *all* forms of Internet voting are vulnerable in points 12-19 below.

These generic attacks are *fundamental*, meaning that there is no general way prevent them from being perpetrated, and no possibility of them all being resolved in the foreseeable future. It is not just a matter of funding a massive development effort, and the problems will then be resolved. Some of these issues *have no solution* without a major restrictive re-architecting of the Internet and the software ecosystem we all live in, which is not about to happen.

11. Here in points 12-19 are the generic attacks that apply to all forms of Internet voting, including email and FAX.

12. **Voter authentication attack:** In any form of remote voting it is essential to know for certain exactly who is casting a vote. This is required to prevent double voting and to verify eligibility to vote. But there is in general no strong way in today's Internet to reliably identify the voter at the other end of an Internet connection. The usual techniques — pins, passwords, personal information, fingerprints, ink signatures, facial recognition, presentation of passport or driver's license, etc. — are all either too weak, have been compromised on a massive scale by major data breaches we read about all the time, or simply do not work reliably end-to-end over an Internet connection. The one strong voter identification and authentication technique we do know — based on public key cryptography — is not offered by the government as a service to ordinary citizens in the U.S. and won't be any time soon, for both technical and political reasons. The result is that any Internet voter authentication system risks either disenfranchising many voters who cannot adequately authenticate themselves, or allowing an automated system to create lots of fake voters (as has happened to social media companies awash in fake accounts).

13. **Voter authorization attack:** After a remote voter is identified and authenticated, it is necessary to verify that they are a registered voter in the jurisdiction in question, verify that they have not yet voted by Internet or some other means, and determine which precinct they

reside in so they can be given the correct blank ballot. This requires looking up the voter in the voter registration database (VRDB) and making several checks. But what if that VRDB has itself been attacked and compromised? Voters may be denied the right to vote, or be given the wrong ballot. This is not a hypothetical case. We know the Russians attacked the VRDB in almost all states and several major counties in 2016, and in one case (Illinois) exfiltrated almost all of the contents of the entire state's voter registration database. Any attacker with that kind of access also has the ability to *modify* that database, creating widespread electoral havoc, though it appears they did not choose to do so in 2016.

14. **Voting device malware attacks:** Voters who cast their votes over the Internet do so from a computer or mobile device that they own. It is completely out of the control of election officials and cannot be "locked down" or in any way secured by them. If the device is infected with malware designed to affect voting then whenever the voter connects to the voting web site, or sends email to the voting email address, or sends a FAX to the voting FAX number, then the malware can completely control the voter's election participation. Simple malware might just prevent the voter from authenticating properly. More complex malware might throw away a ballot with votes it does not like, while giving the voter feedback that it was transmitted. Alternatively, it might actually change the votes internally, but display on the screen exactly the votes that the voter intends. Then the modified ballot would be the one actually transmitted. Neither the voter nor election officials can detect this without violation of vote secrecy. In addition to doing those things the malware could transmit to a third party (a) the voter's identity, (b) the votes that the voter intended to cast, and (c) the modified votes that actually were cast. This leaves the voter open to retaliation and can also give a campaign an early heads up about the electronically cast votes *before* they are legally counted. Finally, malware opens the door to

undetectable electronic vote buying and selling.

15. **Spoofing attacks:** There are many ways to trick voters of one demographic or party into sending their votes to a fake web address, or fake email address, or fake FAX number. Those ballots never reach the correct destination, and they do not count, but the voter believes he or she voted properly.

16. **Router / DNS / email infrastructure attacks:** There are numerous ways to attack ballots as *en route* through the Internet towards their destination. The easiest attack is to just prevent the ballot from getting through by modifying routers, or email forwarding servers, or other parts of the Internet infrastructure such as the Domain Name Service (DNS).

17. **Distributed denial of service attacks:** An election conducted over the Internet can be completely disrupted by a *denial of service* attack. The essence of such an attack would be to send a huge volume of fake ballots to the same web site, or email address or FAX number as the real ballots are supposed to go. The purpose of the fake ballots is not to get them counted, but to clog up the communication channels and/or to keep routers, servers, or firewalls so busy handling and discarding the fake ballots that the real ballots cannot get through. This particular kind of attack is so routine that there are illicit businesses around the world who will conduct such an attack for you for a price.

18. **Server penetration attacks:** The web server or email server or FAX server that receives ballots through the Internet can be penetrated by attackers who can gain control of it and either throw away ballots, add ballots, modify ballots, of just cause general havoc in the server so as to completely disrupt the election. No server connected to the Internet is totally safe from a determined adversary who wants to penetrate and remotely control it. A penetration attack on an online voting system was accomplished in a mock election in 2010 by Prof. Alex Halderman and

his colleagues. They had permission to attack a system that was intended for use in the Washington, D.C. general election that year, as a way of testing its security. Not only did Halderman succeed in penetrating the server in Washington from his offices at the University of Michigan, but he replaced all of the ballots with phony ballots and installed modified software that would replace all future ballots cast as well. Along the way he defended the mock election from probes from Iranian IP addresses, and he gained control of the network of security cameras in the data center where the ballots were being collected. Washington, D.C. officials did not realize this had happened for two full days, until the attackers basically gave away the game and let them know. (Needless to say, officials had to scrap plans for using that system in the real election.)

19. **No meaningful recount-ability or auditability:** This last point is not a form of cyberattack, but rather a recognition that the most powerful weapon we have to defend against cyberattacks on elections is the ability to do a meaningful recount or audit of the results of the election against a reliable record of the voters' original choices. Generally this requires a physical paper ballot hand-written by the voters and collected, saved, and protected by election officials. The results of the election can be *audited* by hand counting an appropriate random sample of those ballots. The results can be used to assess statistically whether the election results as determined by scanners and software actually called the winners and losers correctly. If necessary or called for by law, a full hand recount of the hand-marked paper ballots can be done. But no such audit or recount is meaningfully possible without that original hard copy record of the voter's intent marked directly by the voter. All that is possible then is another software recount of ballots whose integrity is questionable because of all of the potential cyberattack modes listed above.

20. Now, in my view *from a security point of view email voting and FAX voting are about the worst forms of voting ever proposed.* This is fundamentally because ordinary email such as voters would use from their home PCs or mobile devices *is not end-to-end encrypted*. The body of the email along with attachments is encrypted, decrypted, and re-encrypted several times along the path from the voter to the receiver. But during the moments when it has been decrypted and before it is re-encrypted, it is completely vulnerable to manipulation by the IT staff if the companies running the email services, e.g. Google, Microsoft, Yahoo, or the voter's employer (if voting from the employer's computer). This lack of end-to-end encryption has disastrous security consequences.

21. Ballots can not only be discarded in flight, as can happen with other modes of Internet voting, but can be freely modified in flight to reflect the attacker's choices. Any IT person in charge of a mail forwarding server can do this, as well as any remote attacker from anywhere in the world who chooses to hack into one of those servers. Furthermore it is easy for an attacker to select, out of the millions of email messages being transmitted, exactly those that contain ballots, because they (and only they) are sent to the official email address(es) used for collecting ballots. A similar comment can be made about FAX ballots. This kind of attack has actually been demonstrated (not that it was necessary) by Joe Kiniry of Galois, whose associates hacked a home router and inserted malware so that an ballot passing through it was modified on its way to the vote server. There is no fundamental protection against this at all, and no way to detect that it has happened without violating vote secrecy.

22. At moments when they are unencrypted email of FAX ballots can be read or copied in flight by anyone with control of an email forwarding server through which the ballot it passes. There are several serious consequences of this:

(a) Vote privacy is completely lost, because the voter's name and email address of FAX number are attached to the voted ballot.

(b) The loss of vote privacy enables large scale vote buying and selling schemes, or coercion.

(c) Many people have their email service through their employer's infrastructure, and employers generally have the legal right to inspect and archive all email sent to or from employees through company infrastructure. This includes military personnel who would vote in through military networks.

(d) Emailed and FAXed ballots can be copied to third parties in flight. This would be valuable for domestic political operatives who want to know exactly who is voting for what or who want count the votes early to see how to invest their campaign resources during the last days of a campaign while balloting is in progress.

23. Email and FAX headers are totally forgeable and modifiable. The *From:*, *To:* and *Date:* headers are totally forgeable. It is easy to send email that appears to come from someone else. (Spammers do it all the time.) And it is easy to modify the dates on email to make it appear that emailed ballots sent after the close of the election were sent earlier (and thus should be counted in states where the sending date is the criterion used).

24. PDF can be used to deliver malware to the server. Most email voting systems require the ballot and the user's identification to be in the form of PDF attachments to the email message. However, PDF is a notoriously dangerous file type because specially constructed PDF files can be used to deliver malware to whoever receives and opens it. An attacker could create a malicious PDF file that looks like a benign ballot but contains malware. When it reaches the election server it could introduce a backdoor for the attackers to penetrate and gain control of the

election server.

25. Many people seem to have the naïve intuition that if mail-in voting of physical paper ballots is secure enough for use in a public election, then email voting must be also. Nothing could be farther from the truth. As I said, email (and FAX) voting can be attacked by anyone in the world. The attacks can be automated and at large scale, affecting thousands or tens of thousands of votes across many jurisdictions with no more effort than it takes to affect a handful of ballots. And the attackers can be out of reach of U.S. law. But none of this is true for ordinary paper mail-in ballots. Only a comparative handful of people are in a position to touch more than a handful of mail-in ballots, and such attacks cannot be *automated*. It would take a conspiracy of many people to affect a large number of ballots. And those people would have to be located within the U.S. and would be able to be brought to justice if caught. While *functionally* email and paper mail are analogous, from a security point of view they are worlds apart.

26. For all of the reasons above I believe that widespread use of email or FAX for voting, or indeed any other Internet-based delivery system for ballots, puts the integrity of an election and the national security of the United States at grave risk. And I close by saying that this is not just my opinion. It is the general consensus of the entire computer and election security community worldwide. It is reckless and foolhardy to risk instituting email or FAX voting even in this challenging time of Covid pandemic.

Dated: October 8, 2020
San Ramon, California

David R. Jefferson

David R. Jefferson