Halderman Testimony

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Case 2:22-cv-00677-JJT Document 33 Filed 06/08/22 Page 10 of 38

3. General Vulnerability of Electronic Voting Systems

7. Electronic election equipment is notorious for continuing to be inadequately secure

8. against intrusion even after federal government certification for use. In a 2021 article

9. addressing the issue of errors and vulnerabilities in computer code, three professors of

10. computer science cited voting machines as the best-documented example" of

11. adversarial testing" finding "flaws in software that had been certified by outside parties."

12. Steven M. Bellovin et al., Seeking the Source: Criminal Defendants ' Constitutional Right

13. to Source Code, 17 Ohio St. Tech. L. J. 1, 35 (Dec. 2020) (Parker Decl. "8 & Ex. G).

14. «[Outside auditors," they wrote, "have always found flaws" in voting machine software.

15. Id. As a result, "There is broad consensus among elections experts that modern software

16. systems are, by virtue of their design, too complex and unreliable to be relied upon for

17. determining the outcomes of civil elections." Id. at 36-37.

18. A fourth professor of computer science testified in detail about these

19. vulnerabilities before the Senate Select Committee on Intelligence in 2017. J. Alex

20. Halderman, who had spent a decade studying electronic voting systems, testified that "our

21. highly computerized election infrastructure is vulnerable to sabotage and even to cyber

22. attacks that could change votes." He testified, "I know America's voting machines are

23. vulnerable because my colleagues and I have hacked them repeatedly as part of a decade

24. of research studying the technology that operates elections and learning how to make it

25. stronger. We've created attacks that can spread from machine to machine, like a computer

26.

1. virus, and silently change election outcomes. We've studied touchscreen and optical scan

2. systems, and in every single case we found ways for attackers to sabotage machines and

3. to steal votes. These capabilities are certainly within reach for America's enemies.?

4. Russian Interference in the 2016 U.S. Elections at 72, Hearing of S. Sel. Comm. on

5. Intelligence, S.Hrg. 115-92 (June 21, 2017) (Parker Decl. 9 & Ex. H) ("Halderman

6. Testimony"). Professor Halderman testified, "Cybersecurity experts have studied a wide

7. range of U.S. voting machines--including both DREs and optical scanners- and in every

8. single case, they've found severe vulnerabilities that would allow attackers to sabotage

9. machines and to alter votes. That's why there is overwhelming consensus in the

10. cybersecurty and election integrity research communities that our elections are at risk."

11. Id. at 76 (emphasis in original).

12. On August 2, 2021, Professor Halderman signed a declaration for litigation

13. concerning electronic voting systems used in Georgia. The declaration stated that

14. Professor Halderman had spent twelve weeks performing intensive testing of Dominion

15. voting equipment used in Fulton County, Georgia, and found "multiple severe security

16. flaws." that attackers could exploit "to install malicious software, either with temporary

17. physical access (such as that of voters in the polling place) or remotely from election

18. management systems," and "such malware, once installed could alter voters' votes while

19. subverting all the procedural protections practiced by the State." Decl. of J. Alex

20. Halderman 4, Curling v. Raffensperger, no. 17-cv-2989-AT, ECF 1304-3 (N.D. Ga.

21. Feb. 3, 2022) (Parker Decl. "10 & Ex. I).

22. After hearing Dr. Halderman's testimony and a large amount of other evidence,

23. the federal court in the Curling litigation concluded, "Evidence presented in this case

24. overall indicates the possibility generally of hacking or malware attacks occurring in

25. voting systems and this particular system through a variety of routes - whether through

1. physical access and use of a USB flash drive or another form of mini-computer, or

2. connection with the internet. As discussed in the declarations and testimony of the
3. proffered national cybersecurity experts in this case, a broad consensus now exists among
4. the nation's cybersecurity experts recognizing the capacity for the unobserved injection
5. of malware into computer systems to circumvent and access key codes and hash values
6. to generate fraudulent codes and data. In these experts' views, these risk issues are in play
7. in the operation of Dominion's Democracy Suite 5.5-A GA." Curling v. Raffensperger
8. 493 F. Supp. 3d 1264, 1280 (N.D. Ga. 2020).
9. Douglas Logan is an industry cybersecurity practitioner who has developed
10. cybersecurity programs and led cybersecurity-related services for the federal government
11. and Fortune 500 corporations, including malicious code detection, code review, threat
12. modeling, and hacking vulnerability testing. Logan Decl. 19 3-5. He has also written
13. training materials and taught classes on these topics. Id. 6. He has overseen or conducted
14. application vulnerability assessments on over 2,000 software applications. Id. 18. Logan
15. testifies:
16. Commercially available voting machines from major vendors have for years been
17. hacked by participants at an annual cybersecurity conference called DEFCON,
18. including by participants with little prior knowledge and limited tools and
19. resources. Id. T9 43-47. A variety of techniques have been demonstrated to allow
20. an unauthorized person to change votes within the electronic election equipment,
21. even new systems. Id. 147. The vulnerability to hacking includes equipment with
22. a security vulnerability that was disclosed to the vendor a decade ago, yet never
23. fixed by the manufacturer. Id. T45.
24 • Investigation of Dominion equipment used to administer the 2020 election in
25. Antrim County, Michigan revealed that the election software could be easily
26

modified to attribute one candidate's votes to another candidate, the election software fell short of basic validation practices used even in commercial inventory control software, and the software could easily be intentionally modified to wrongly attribute votes to a favored candidate while outputting manipulated results on the poll tape, thereby leaving little indication that anything had been tampered with. Id. 1948-54. After analyzing equipment used in Antrim County, post-election, Logan found the Dominion software exhibited a large number of failures in implementing secure coding practices, application security design principles. and cyber security best practices. Id. "57.

Logan authored an evaluation, commissioned by the Arizona Senate, of the performance of Maricopa County, Arizona voting practices and equipment during the 2020 general election. Id. T1 10, 59. After reviewing the Dominion equipment and software used by Maricopa County, he concluded the software lacked necessary security measures; security logs that recorded access to the system had been lost and files deleted, often without any record of who performed these actions; and the system allowed multiple people to access it through shared accounts that did not change from year to year, thereby permitting changes to be made without any record of who made the changes. Id. - 59-63 & Ex. E.

"Air gap" cyber security practices are not sufficient to adequately protect election systems. Id. 9 81-84. First, there is substantial evidence that many election systems are not actually protected by air-gapping at all times. Id. 182. Second. even a properly air-gapped system can have malicious code copied to it through means other than a direct network connection, such as through a portable USB drive. Id. IT 83-84.

1. After speaking with election workers across the country, Logan concluded that
2. many election workers operating electronic equipment to administer elections have
3. inadequate technical knowledge and rely fully on the equipment vendor or its
4. subcontractors to perform the most basic tasks. Id. 19 12, 87-88.
5. Considering the complexity of electronic election equipment and software, the
6. general lack of cybersecurity sophistication of election workers, elected officials,
7. and others, and the equipment's vulnerability to compromise, Logan has
8. concluded that electronic voting systems cannot be properly secured by the 2022
9. elections and should not be used. Id. « 85-91.
10. Col. (Ret.) John Mills served in senior positions in the Department of Defense,
11. including Director of Cybersecurity Policy, Strategy, and International Affairs. Mills
12. Decl. M 2, 21. He has taught cybersecurity law and policy at the University of Maryland
13. since 2013. Id. "2. He has also served as an election official at the county level. Id. 9 17.
14. 22. Col. Mills testifies that "remote access operations" capability to access computer
15. networks without detection have greatly expanded from the 1980s to the present. Id. 19 4-
16. 6, 27-45. The U.S. Government conducts remote access operations. Id. 97. Other
17. countries, organizations, and individuals have capabilities to conduct remote access
18. operations with varying degrees of sophistication, which have expanded at an accelerating
19. rate over the last two decades. Id. " 8. Electronic election infrastructure can be subjected
20. to remote access operations that can change vote totals. Id. 9 9-10. Today, remote access
21. operation capabilities have "escaped" from U.S. "classified environments" into "the
22. wild," and other countries including China, Russia, Iran, North Korea, and Venezuela
23. now use the same, similar, and improved methodologies. Id. 1911, 15, 36. In view of
24. successful cyberattacks now known to have succeeded against U.S. federal government
25. targets and the state of the U.S. election process, Col. Mills concludes that federal
26

1. government assertions about the 2020 election being "the most secure in American

2. history" have "little, if any, basis in fact." Id. 1918-19. American elections deviate

3. substantively from the standards for free and fair elections, with respect to the operation

4. of election machines and technology. Id. 19 46-48. After reviewing evidence concerning

5. the election equipment used in Mesa County, Colorado for the 2020 election, Col. Mills

6. finds the evidence "consistent with previous, publicly known, computer network

7. intrusions, breaches, exfiltrations, and compromises of data integrity conducted via

8. remote access operations by sophisticated actors, likely nation state level, with intimate.

9. insider knowledge of the machines, networks, operating systems, and complete

10. architecture of the information technology environment including off premise, 'cloud

11. based storage and processing." Id. T9 12-13, 20-21

4. Supply Chain Vulnerability of Electronic Voting Systems

13. Yet another vulnerability in electronic election equipment is vulnerability to attack

14 through the supply chain that produces the hardware and software used in the equipment.

15. Shawn Smith is a retired U.S. military officer who served more than 25 years performing

16. tasks related to the management of computer-based weapons systems, and who has served

17. in his retirement as a consultant to the Department of Defense concerning cyber threat

18 risks against U.S. governmental and non-governmental national security targets. Smith

19. Decl. 19 2-6. Smith testifies that *U.S. elections are critically vulnerable to exploitation

20. by foreign adversaries through supply chain compromise of our computerized election

21. systems." Id. T8. A supply chain compromise is the deliberate introduction of flaws.

22. covert access or functionality, malicious code, or other undesirable attributes into a

23. product or service in the supply chain lifecycle of the product or service. Id. \ 12. A supply

24. chain compromise may be intended to make a device accessible to unauthorized parties

25. or to behave differently upon the occurrence of a command or specified conditions. Id. It

Case 2:22-cv-00677-JJT Document 33 Filed 06/08/22 Page 14 of 38

1. government assertions about the 2020 election being "the most secure in American

2. history" have "little, if any, basis in fact." Id. 1918-19. American elections deviate

3. substantively from the standards for free and fair elections, with respect to the operation

4. of election machines and technology. Id. 19 46-48. After reviewing evidence concerning

5. the election equipment used in Mesa County, Colorado for the 2020 election, Col. Mills

6. finds the evidence "consistent with previous, publicly known, computer network

7. intrusions, breaches, exfiltrations, and compromises of data integrity conducted via

8. remote access operations by sophisticated actors, likely nation state level, with intimate.

9. insider knowledge of the machines, networks, operating systems, and complete

10. architecture of the information technology environment including off premise, 'cloud

11. based storage and processing." Id. T9 12-13, 20-21

End of section