The University of New Hampshire Law Review

Volume 21 | Number 2 Article 9

3-1-2023

Is Internet Voting Trustworthy? The Science and the Policy Battles

Andrew W. Appel

Andrew W. Appel

Is Internet Voting Trustworthy? The Science and the Policy Battles

21 U.N.H. L. Rev. 523 (2023)

ABSTRACT. According to clear scientific consensus, no known technology can make internet voting secure. In some applications—such as e-pollbooks (voter sign-in), voter registration, and absentee ballot request—it is appropriate to use the internet, as the inherent insecurity can be mitigated by other means. But the insecurity of paperless transmission of a voted ballot through the internet cannot be mitigated.

The law recognizes this in several ways. Courts have enjoined the use of certain paperless or internet-connected voting systems. Federal law requires states to allow voters to use the internet to request absentee ballots but carefully stops short of internet ballot return (i.e., voting).

But many U.S. states and a few countries go beyond what is safe: they have adopted internet voting for citizens living abroad and (in some cases) for voters with disabilities.

Most internet voting systems have an essentially common architecture, and they are insecure at least at the same key point: after the voter has reviewed the ballot but before it is transmitted. I review six internet voting systems deployed between 2006 and 2021 that were insecure in practice, just as predicted by theory—of which some were also insecure in surprising new ways, "unforced errors".

We cannot get along without the assistance of computers. U.S. ballots are too long to count entirely by hand unless the special circumstances of a recount require it. So computer-counted paper ballots play a critical role in the security and auditability of our elections. But audits cannot be used to secure internet voting systems, which have no paper ballots that form an auditable paper trail.

There are policy controversies: trustworthiness versus convenience, and security versus accessibility. From 2019 to 2022 there were lawsuits in Virginia, New Jersey, New York, New Hampshire, and North Carolina; legislation enacted in Rhode Island and withdrawn in California. There is a common pattern to these disputes, which have mostly resolved in a way that provides remote accessible vote by mail (RAVBM) but stops short of permitting electronic ballot return (internet voting).

What would it take to thoroughly review a proposed internet voting system to be assured whether it delivers the security it promises? Switzerland provides a case study. In Switzerland, after a few years of internet voting pilot projects, the Federal Chancellery commissioned several extremely thorough expert studies of their deployed system. These reports teach us not only about their internet voting system itself but about how to study those systems before making policy decisions.

Accessibility of election systems to voters with disabilities is a genuine problem. Disability-rights groups have been among those lobbying for internet voting (which is not securable) and other forms of remote accessible vote by mail (which can be adequately securable). I review statistics showing that internet voting is probably not the most effective way to serve voters with disabilities.

I. THE SUBSTANTIVE RIGHT TO VOTE IS NOT FURNISHED BY A VOTING SYSTEM THAT IS HACKABLE SO THAT A SINGLE ACTOR CAN CHANGE VOTES UNDETECTED AT LARGE SCALE

In a paperless computer-based voting system, voters indicate their choice of candidates through a computer-based user interface (touchscreen, or screen with keyboard, or screen with buttons, or audio interface). The computer program records the votes and stores them, transmits them, and/or tallies them.

Whether the computer is embedded in a special-purpose voting machine or is the voter's own laptop or smartphone, it is a fully general-purpose computer capable of running any software. On that same computer hardware, a malicious actor could install fraudulent software that records systematically different votes than what the voter selected, while giving misleading feedback to the voter that the selected votes are being recorded.

Courts in New Jersey and Georgia, as I will explain, have recognized that paperless computer-based voting systems, because the votes are recorded entirely at the discretion of whatever software happens to be installed, are so insecure that it they are unconstitutional.[1]

Advocates sued New Jersey in 2004 (in State court, on State constitutional grounds),[2] and Georgia in 2017 (in Federal court, on Fourteenth Amendment grounds),[3] seeking injunctions barring those States' use of paperless direct-recording voting machines. In both cases, plaintiffs argued that such systems are so inherently insecure that they impair the substantive right to vote.[4] In both cases, the courts denied State defendants' motions to dismiss; both cases went to trial (New Jersey in 2009, Georgia in 2019).[5]

New Jersey and Georgia used different makes and models of direct-recording (DRE) voting machines.[6] In both cases, the voting machines are freestanding and

---

[1] *See generally* Gusciora v. McGreevey, 929 A.2d 599, 599 ((N.J. Super. Ct. App. Div. 2006)); , rev'd sub nom. Gusciora v. Corzine, No. MER-L-2691-04, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *1 (Feb. 1, 2010); Gusciora v. Christie, No. A-5608-10T3, 2013 N.J. Super. Ct. App. Div. LEXIS 2278, at *1 (Sept. 16, 2013); Curling v. Raffensperger, 397 F. Supp. 3d 1334, 1339 (N.D. Ga. 2019).

[2] *Gusciora,* 929 A.2d 599 at 599; *Gusciora* , 2013 N.J. Super. Ct. App. Div. LEXIS 2278, at *1.

[3] *See Curling*, 397 F. Supp.3d 1334 at 1339.

[4] *See Gusciora,* 929 A.2d at 599*; Curling*, 397 F.Supp.3d at 1353.

[5] *See Gusciora,* 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *3; Curling*, 397 F.Supp.3d at 1337.

[6] *See Gusciora,* 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at*2*; Curling*, 397 F.Supp.3d at 1338. *See also The Verifier – Election Day Equipment – November 2024*, THE VERIFIER, https://verifiedvoting.org/verifier [https://perma.cc/APQ9-Y687] (a database published by the

not directly connected to the internet, but the election-management systems (EMS) that managed them were internet-connected.[7]

In New Jersey in 2010, the Court found that a hacker could indeed replace the software in the DRE voting system to make it cheat.[8] But the Court was not convinced that a hacker would have sufficient access to the system and did not enjoin use of the machines.[9] The Court did rule that election systems must not be connected to the internet—on the basis of testimony about insecurities and vulnerabilities of the EMS computers.[10]

In Georgia, the Federal District Court in 2019 did enjoin[11] the use of paperless DRE voting machines. By the 2020 primary and general elections, the State of Georgia had switched to a paper-based system on which voters use a computer to mark paper ballots and have the opportunity to inspect those ballots before depositing them for casting, scanning, and counting.[12]

After the November 2020 election, there was controversy in Georgia about the result of the presidential election.[13] The fact that Georgia had paper ballots in 2020 made it possible to recount the paper ballots and establish the legitimacy of the result.[14] This would not have been possible in any election between 2004 and 2018

Verified Voting Foundation showing what kinds of election machines were used in each U.S. jurisdiction in every election cycle from 2006 to 2022).

7 *See Gusciora*, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *27; *Curling*, 397 F. Supp. 3d 1334 at 1350. In both cases the Courts' opinions discussed the internet-connected nature of the respective election-management systems.

8 *Gusciora*, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *353 ("As long as computers, dedicated to handling election matters, are connected to the Internet, the safety and security of our voting systems are in jeopardy. Therefore, if the State has not done so already, Clerks shall be advised that computers utilized for election-related duties shall at no time be connected to the Internet.").

9 *Id.*

10 *Id.*

11 *Curling*, 397 F. Supp. 3d at 1412.

12 *The Verifier – Election Day Equipment in Georgia – November 2020*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020/state/13 [https://perma.cc/T6W8-YXP5].

13 It is even alleged that on January 2, 2021 a person telephoned the Georgia Secretary of State and urged him to "find 11,780 votes." S*ee* Michael D. Shear & Stephanie Saul, *Trump, in Taped Call, Pressured Georgia Official to 'Find' Votes to Overturn Election*, N.Y. TIMES (Jan. 3, 2021), https://www.nytimes.com/2021/01/03/us/politics/trump-raffensperger-call-georgia.html [https://perma.cc/6HN3-FCHG].

14 *Id.*

when Georgia was using paperless DREs.[15]

Those other states that had been using paperless DREs largely abandoned them by 2018. But polling-place DREs are not internet voting: what scientific principles apply, and what Federal and State laws apply, to the use of the internet in elections?

II. EXPERIMENTS AND ASSESSMENTS: THE DEVELOPMENT OF NATIONAL POLICIES AND LAW ON INTERNET VOTING 2000-2020

By the year 2000, the international internet was well enough developed and familiar enough to the public that a few countries experimented with voting by internet for citizens living abroad.[16] This class of citizens suffered from slow international mail service that hindered traditional absentee balloting. In the U.S., the Federal Voting Assistance Program (FVAP) of the Department of Defense commissioned in 2004 the Secure Electronic Registration and Voting Experiment (SERVE).[17] In France, the *Assemblée des Français de l'étranger*[18] started in 2006 using an internet voting system. Estonia adopted internet voting in 2005 for municipal election and in 2007 for parliamentary elections.[19]

Computer scientists and cybersecurity experts analyzed these systems and explained how internet voting systems are inherently insecure.[20] In particular, the 2004 SERVE Report[21] explained how the FVAP's SERVE system was vulnerable: how an attacker could control the voter's computer, and how the attacker could exploit that to cast fraudulent ballots. The report concluded that FVAP (and its contractors)

---

[15] *The Verifier – Election Day Equipment in Georgia – November 2020*, *supra* note 12.

[16] *See infra* Section VI.

[17] *See* David Jefferson et al., *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, 1, 4 (Jan. 21, 2004) https://classes.cs.uoregon.edu/04W/cis607ev/readings/SERVE_paper.pdf [https://perma.cc/4E7K-JHNM].

[18] The *Assembly of French Citizens Abroad*, which in turn elects 12 members of the regular French Senate. *See* Andrew Appel, *Ceci N'est Pas Une Urne: On the Internet vote for the Assemblée des Français de l'Étranger*, 1, 3 (June 14, 2006), *https://www.cs.princeton.edu/~appel/papers/urne.pdf* [https://perma.cc/3Z3P-9UYJ].

[19] Drew Springall et al., *Security Analysis of Estonian Internet Voting System*, CCS '14: PROCEEDINGS OF THE 2014 ACM SIGSAC CONF. ON COMPUT. AND COMMC'N SEC., 703, 703 (2014).

[20] *See* Jefferson et al., s*upra* note 17 at 21. This was the minority report of a 10-member expert panel that FVAP assembled to evaluate SERVE. The full peer review group did not issue a final report.

[21] *See id.* This was the minority report of a 10-member expert panel that FVAP assembled to evaluate SERVE. The full peer review group did not issue a final report.

had "been aware of [these] security problems" and used "engineering sophistication and skill" in "attempts to ameliorate and eliminate them."[22] The problem was that in 2004 "a secure, all-electronic remote voting system" was "an essentially impossible task."[23]

"Because DOD did not want to call into question the integrity of votes that would have been cast via SERVE, they decided to shut it down prior to its use by any absentee voters."[24] DOD's Federal Voting Assistance Program concentrated on improving remote absentee balloting in other ways.[25]

Reports on the French[26] and Estonian[27] systems drew similar conclusions, but those countries continue to use internet voting today (France only for overseas citizens). As I will discuss below, in 2022 "a secure, all-electronic remote voting system" is still impossible with today's technology.

Federal legislation in 2010, the *Military and Overseas Voter Empowerment Act (MOVE),* required state and county election officials to provide internet access for overseas voters: online voter registration and requests for absentee ballots, electronic delivery of blank ballots to voters, and online tracking systems for returned ballots.[28] But the MOVE act did not require states to permit the electronic return of voted ballots, perhaps because legislators had come to understand that this was essentially impossible to make secure.[29]

Federal law largely does not regulate the choices states make regarding voting machines or electronic voting technology. Although the Constitution gives Congress the power to regulate the "time, place, and manner" of congressional elections, Congress has chosen a voluntary system for regulating voting technology.[30] The Election Assistance Commission (EAC) specifies Voluntary

---

[22] *See id.*

[23] *See id.*

[24] U.S. GOV'T ACCOUNTABILITY OFF., GAO-06-521, ELECTIONS: ABSENTEE VOTING ASSISTANCE TO MILITARY AND OVERSEAS CITIZENS INCREASED FOR THE 2004 GENERAL ELECTION, BUT CHALLENGES REMAIN (2006).

[25] *See generally* FEDERAL VOTING ASSISTANCE PROGRAM, fvap.gov [https://perma.cc/D26M-WTA3].

[26] Appel, *supra* note 18 at 3.

[27] Springall et al., *supra* note 19 at 703.

[28] Military and Overseas Voter Empowerment Act, Ind. Code Ann. § 3-11-4-5.7.

[29] Military and Overseas Voter Empowerment Act § 3-11-4-5.7.

[30] U.S. CONST. art. 1, § 4. An exception to this general rule of "Federal law imposes mostly voluntary restrictions on voting-machine technologies that states can adopt" is that mechanical lever machines and punch-card voting systems were both banned by the Help America Vote Act of

Voting Systems Guidelines (VVSG); many of the states either formally or informally require that the machines they adopt comply with the VVSG.[31] But the VVSG do not cover internet voting systems.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issues reports and fact sheets about voting security, including use of the internet, which the states are free to use or ignore—for example, CISA advises that no current technology can mitigate the high risk inherent in electronic ballot return.[32]

So, in summary of the developments described above, Federal law requires the states to provide online services in connection with voter registration and absentee ballot request, but federal law does not require the states to provide internet voting, and Federal Agencies explicitly discourage the states from permitting internet voting.

By 2022, thirty states[33] permitted some form of internet voting (electronic return of voted ballots) for "UOCAVA voters;" that is, citizens in the military or living abroad as defined by the Uniformed and Overseas Citizens Absentee Voting Act of 1986.

In the last few years, after intensive lobbying and lawsuits by the American Federation for the Blind, several states have extended or considered extending the same forms of internet voting to in-state citizens with disabilities.[34] There has been pushback from election-security advocates who say that such systems are too insecure to be trusted.[35] It is not at all clear that this is the form of voting wanted by most voters with disabilities. Below I will discuss several lawsuits and legislative battles in this arena.

2002, Pub. Law No. 107-252, 116 Stat. 1666.

[31] Each state's legislature sets out the requirements for what kinds of voting machines are acceptable. Most states delegate to the Secretary of State or other State Election Director the power to determine whether a particular vendor's machine satisfies these criteria. In some states the chief election official is advised by a statutory committee. There are two potential problems: statutes about voting machines (many dating from 100 years ago and amended from time to time) may not have envisioned the Internet; and Secretaries of State (and their statutory advisers) may not have the cybersecurity expertise to evaluate modern voting systems.

[32] Cybersecurity And Infrastructure Sec. Agency, Critical Infrastructure Security and Resilience Note: Mail-In Voting In 2020 Infrastructure Risk Assessment 8 (2020).

[33] *See* Henry D. Herrington, Ballot Acrobatics: Altering Electronic Ballots using Internal PDF Scripting (Apr. 25, 2022) (A.B. thesis, Princeton University) (on file with author).

[34] *See infra* Section XV.

[35] *See* infra Section XV.

III. TERMINOLOGY

"Internet voting" is any system that sends marked (voted) ballots through the internet to election management computers that will tabulate them without also sending a paper ballot from the voter's possession to the election authority.[36] That is, "internet voting" is the paperless return of a marked ballot from a voting terminal or from the voter's own computer (or phone), via the internet or a network connected to the internet, to computer servers that tabulate the votes.

A "paper ballot" system is one in which a marked paper ballot in the voter's possession, which the voter can review by physical inspection, is physically transmitted to a physical ballot box from which it can be recounted by physical inspection. A system in which a paper ballot is printed in a place or manner that the voter cannot physically review it is not a "paper ballot" system.[37]

"Online voter registration" is not internet voting. "Online absentee ballot request" is not internet voting.

"Remote Accessible Vote By Mail" (RAVBM) is a widely used term that describes a variety of procedures and methods by which voters with disabilities may vote from home.[38] RAVBM may include the download of blank (unvoted) ballots from election servers to the voter's own computer for the voter to mark at home, then print, and (physically) mail.[39] This is not internet voting. An RAVBM system may allow voters to use an app on their computer to mark the ballot before printing and mailing it.[40] This is not internet voting. Some RAVBM systems allow the voter to return their ballot (by e-mail or upload) as an electronic message over the internet.[41] That *is* internet voting.

---

[36] NAT'L ACADS. OF SCI., ENG'G, & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 106 (The Nat'l Acads. Press 2018).

[37] *Id.* A system in which the ballot tabulated in a recount is not the same sheet of paper that the voter physically reviewed is not a "paper ballot" system. The word "paperless", used throughout this article, refers to any system that is not a paper ballot system. Hence, for example, a system in which the voter's selection of candidates is transmitted over the internet to a place where it is printed on paper is a "paperless" system.

[38] *Remote Accessible Vote-By-Mail (RAVBM)*, CAL. SECRETARY OF STATE: SHIRLEY N. WEBER, PH.D., https://www.sos.ca.gov/elections/voting-resources/remote-accessible-vote-mail [https://perma.cc/SFG5-MMNQ].

[39] *Id.*

[40] *Id.*

[41] *See infra* Section XV.

IV. THE CLEAR SCIENTIFIC CONSENSUS IS THAT INTERNET VOTING IS NOT SECURABLE

In 2004 the SERVE report said, "a secure, all-electronic remote voting system" was "an essentially impossible task."[42]

In 2018 the National Academies of Science, Engineering, and Medicine consensus study report said:

> 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.[43]

NASEM consensus studies are written by committees of scientific experts (in this case also including law professors and election officials) who are tasked with holding hearings and then reporting the scientific consensus; their reports are peer-reviewed before publication.

In 2020 CISA advised that

> Electronic ballot return is high risk. Electronic ballot return, the digital delivery of a voted ballot back to the election authority, faces significant security risks to voted ballot integrity, voter privacy, and system availability. There are no compensating controls to manage electronic ballot return risk using current technologies. While many risks associated with electronic ballot return have a physical analog with the risk associated with the mailing of ballots, the comparison can miss that electronic systems provide the opportunity to rapidly affect voting at scale.[44]

The science on this question is stable: no miraculous new technologies have appeared to make internet voting secure. "The opportunity to rapidly affect voting at scale" means, for example, a single actor in Pakistan or Pennsylvania; or in Moscow, Russia or Moscow, Idaho; could remotely hack server computers or voters' computers and alter thousands or millions of votes. Such threats are unlike the threats to paper ballots: physical paper ballots can be attacked (e.g., by stealing ballot boxes), but those attacks cannot be done remotely or undetectably at massive scale by a single actor; and local physical attacks can be defended by local chain-of-custody practices that are understandable to local officials and citizens.

---

42 *See* Jefferson et al., *supra* note 17, at 3.

43 NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 6–7.

44 CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, *supra* note 32 at 8.

V. THE SUBSTANTIVE RIGHT TO VOTE IS NOT FURNISHED BY A VOTING SYSTEM THAT IS HACKABLE SO THAT A SINGLE ACTOR CAN CHANGE VOTES UNDETECTED AT LARGE SCALE

The science is clear. The server computer that counts the votes, and the voter's own computer on which the voter prepares and transmits a ballot, inevitably will have security vulnerabilities that can allow an attacker to alter votes.

Why are security vulnerabilities inevitable in practice? Twenty-first century computers are extremely complex, with many layers of hardware (as I will explain) and millions of lines of software. These layers are susceptible to design mistakes—bugs. Some of these bugs are *exploitable security vulnerabilities* that leave the computer vulnerable to attack. The attack (typically) comes in the form of unexpected input provided by the attacker, which confuses the software into running programs supplied by the attacker.[45] These attacker-supplied programs can perform all manner of malicious acts, such as altering votes in an organized way as designed by the attacker.

Major platforms such as Apple's iOS smartphone operating system and Google's Android smartphone operating system are designed by large sophisticated companies who have every incentive to make secure systems without exploitable bugs—and yet there continue to be about twenty-five exploitable vulnerabilities found per year in iOS and about 100 per year in Android.[46] Many vulnerabilities are also found each year in desktop operating systems, such as Windows and MacOS, and server operating systems, such as Linux.[47] Smaller companies (such as voting system vendors) have a smaller staff of cybersecurity engineers and should be expected to have a higher rate of security vulnerabilities per line of source code.

Many of these vulnerabilities are classed as *remotely exploitable:* that is, an attacker anywhere on the internet could use the bug/vulnerability to burrow into the voter's computer or phone and control its behavior.[48]

A modern computer (desktop, server, or smartphone) has many layers of software:[49]

---

[45] This is basic computer science since 1988.

[46] Based on my analysis of the CVE database, 2018-2020, published by CVE.org. CVE is an organization (originally the Common Vulnerability Enumeration) that collects and publishes vulnerability reports; it has been funded since 1999 by (at various times) over a dozen Federal agencies and departments.

[47] Appel, *supra*, note 18 at 8.

[48] "Remotely exploitable" is a standard term in computer science, with this meaning.

[49] *See generally* NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36. To further explain *why* modern systems have so many layers of such monstrous complexity, then this is a good

- The topmost layer is the ***application:*** calendar, word-processing, photography, or voting. Too often, analyses of voting system security focus on the voting app and neglect the lower layers.
- The application is supported by a ***run-time system*** that provides services to the application, such as memory management and input-output buffering.
- This runs as the client of an ***operating system*** (such as MacOS, Windows, Linux, iOS, and Android) that manages and controls the execution of the application.
- The OS is loaded by a ***BIOS*** *(Basic Input-Output System)* or ***UEFI*** *(Unified Extensible Firmware Interface)*, which is responsible for fetching the OS from disk and starting it up. Also at this layer is usually a "management engine" (such as ***IME***, Intel Management Engine) that allows (e.g.,) corporate IT staff to take control of the computer for (e.g.,) operating-system upgrades—but which could also be exploited by attackers.
- At these low levels are also ***device drivers***, such as the software that manages the USB interface (for thumbdrives, etc.), the disk controller (for internal hard drives), and the network controller (for wi-fi, etc.).

The software at each of these levels is thousands, or millions, or hundreds of millions of lines of source code.[50] This source code is written by human beings who find it difficult to envision all the circumstances in which their program might run. It is not surprising that in those hundreds of millions of components there are bugs.

Each of these layers has control over the layer above it. That is, the operating system decides which application program to run.[51] The OS is *supposed* to run the program requested by the user but (if maliciously hacked) might choose to run a

---

explanation: Thomas Dullien, *Keynote Address at The 10th Int'l Conf. on Cyber Conflict (CyCon), organized by NATO: Security, Moore's Law, and the Anomaly of Cheap Complexity*, YOUTUBE (June 2018), https://www.youtube.com/watch?v=q98foLaAfX8 [https://perma.cc/4S8K-QS2A].

[50] *See e.g.*, *One Windows Kernel*, MICROSOFT, https://techcommunity.microsoft.com/t5/windows-os-platform-blog/one-windows-kernel/ba-p/267142 [https://perma.cc/8SD8-J9QT]; *Linux kernel 27.8 million*, LINUX, https://www.linux.com/news/linux-in-2020-27-8-million-lines-of-code-in-the-kernel-1-3-million-in-systemd/ [https://perma.cc/M38S-ZERU]; *Chromium (Google Chrome)*, SYNOPSYS, https://www.openhub.net/p/chrome/analyses/latest/languages_summary [https://perma.cc/9JUT-38JR]; *eXtensible Host Controller Interface for Universal Serial Bus*, INTEL, https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/extensible-host-controler-interface-usb-xhci.pdf [https://perma.cc/N8X3-BKH7].

[51] *See* NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 89—90.

fraudulent application.[52] And when running an application (fraudulent or not), a hacked operating system, when serving requests from the layer above, might choose to give fraudulent answers that deliberately confuse the upper layer into doing specific bad acts.[53] The same holds for the device drivers servicing the OS (and UEFI and IME underneath): A maliciously hacked lower layer can corrupt the operation of the upper layers, not at random but in a way designed by the attacker.[54]

Therefore, even if one were to carefully inspect the voting application program and conclude that it accurately counts the votes, one can never be sure that the lower layers (if hacked) are actually running *that* voting app, and not some fraudulent replacement for it.

VI. INTERNET VOTING SYSTEMS ARE INCSECURE NOT ONLY IN THEORY: EACH DEPLOYED SYSTEM IS INSECURE IN ITS OWN WAY

The National Academies study and the CISA advisories say that internet voting is inherently insecure.[55] But are specific internet voting systems actually insecure in practice?

- In 2010, the District of Columbia deployed an internet voting system for city elections.[56] Prior to the election, they operated a mock election to allow the public to test its functionality and security.[57] Within 48 hours, academic researchers took complete control of the server, with full ability to install fraudulent voting software.[58] They notified the District and described the security flaws in a scientific paper.[59] D.C. abandoned internet voting.[60]
- Estonia introduced internet voting in 2005.[61] Academic researchers in 2014 found that the I-voting system has "serious architectural limitations and procedural gaps" and demonstrated (on a reproduction

---

52 *Id.*

53 *Id.*

54 *Id.*

55 *Supra* Section IV.

56 Sarah Wheaton, *Voting Test Falls Victim to Hackers*, N.Y. TIMES (Oct. 8, 2010), https://www.nytimes.com/2010/10/09/us/politics/09vote.html [https://perma.cc/TS3H-JMWE].

57 *Id.*

58 *Id.*

59 *See generally* Scott Wolchok et al., *Attacking the Washington, D.C. Internet Voting System*, 27 FIN. CRYPTOGRAPHY AND DATA SEC. 114 (2012).

60 Wheaton, *supra* note 56.

61 *See* Springall et al., *supra* note 19, at 703—15.

of the system) how attackers could target servers or voter's computers to alter election results.[62] Estonia continues to use I-voting.[63]

- The Australian state of New South Wales deployed an iVote system in 2015. [64] Academic researchers "uncovered severe vulnerabilities that could be leveraged to manipulate votes, violate ballot privacy, and subvert the verification mechanism."[65] NSW continues to use successors of the iVote system, which are still insecure.[66] In addition to being insecure, it suffers from other problems: thousands of voters could not access iVote to cast their ballots on election day.[67] The NSW Supreme Court subsequently voided three municipal elections whose results were decided by a smaller margin than the number of lost votes.[68]
- Switzerland deployed an internet voting system in 2019.[69] Academic researchers immediately found severe security flaws.[70] Switzerland commissioned a formal expert study (which I discuss below), then suspended the use of this system.[71]
- West Virginia deployed the Voatz internet voting system in 2020 for use by UOCAVA voters.[72] Academic researchers immediately found severe security flaws.[73] West Virginia discontinued the use of Voatz

---

[62] *See id.*

[63] *See id.*

[64] J. Alex Halderman & Vanessa Teague, *The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election*, 5 E-VOTING AND IDENTITY 35, 35 (2015).

[65] *Id.*

[66] Vanessa Teague, Faking an iVote decryption proof: Why the decryption proof flaw identified in the SwissPost system affects the iVote system too, (Nov. 14, 2019) (unpublished manuscript) (on file with author); Vanessa Teague, *How NOT to Assess an E-voting System*, FREEDOM-TO-TINKER (June 28, 2022), https://freedom-to-tinker.com/2022/06/28/how-not-to-assess-an-e-voting-system/[https://perma.cc/P4SR-F8U8].

[67] Halderman & Teague, *supra* note 64 at 15.

[68] *NSW Electoral Comm'r v. Kempsey Shire Council [No. 2]* (2022) 282 NSWSCR 1(Austl.).

[69] Thomas Haines et al, *How not to prove your election outcome*, IEEE SYMPOSIUM ON SEC. AND PRIV. 644, 644–60 (2020).

[70] *Id.*

[71] *Id.*

[72] Michael A. Specter at al., *The Ballot is Busted Before The Blackchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections,* 29TH USENIX SECURITY SYMPOSIUM 1535, 1535–53 (2020).

[73] *Id.*

and switched to Democracy Live's OmniBallot.[74]

- Several states in 2020 used or considered the OmniBallot internet voting system from Democracy Live for UOCAVA and disabled voters.[75] Academic researchers found severe security and privacy flaws.[76] Some but not all of those states discontinued use of OmniBallot or at least avoided its internet voting features.[77]

Yes, internet voting systems are insecure in both theory and practice.

VII. THE FALLACY OF "NOBODY HACKED US, SO IT MUST BE SECURE"

Vendors and election administrators who deploy internet voting systems sometimes say, nobody has succeeded in hacking into our system, so it must be safe. Or they say, we ran a pilot mock election for three weeks and invited hackers to test it. Neither of these is a reliable way to demonstrate security. If no hack is detected, that could mean that a malicious hacker has taken over your system but you haven't noticed.

"White-hat hackers" (those who break into a system with the intention of ethically notifying the owners of their security weaknesses) may simply not have the time or interest in providing pro-bono services to every different pilot project.[78] Hacking into a computer system may require days or weeks of effort.[79] It is worth the trouble only for the malicious attacker who is trying to change an election with real-world consequences.

---

[74] *Id.*

[75] Micheal Specter & J Alex Halderman, *Security Analysis of the Democracy Live Online Voting System, in* 30TH USENIX SECURITY SYMPOSIUM 3077, 3077–92 (2021).

[76] *Id.*

[77] *Id.*

[78] *White Hat*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/white%20hat [https://perma.cc/6LGK-25KH].

[79] *See* Lillian Ablon & Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND CORP., (2017) https://www.rand.org/pubs/research_reports/RR1751.html [https://perma.cc/B2AD-24TX]. To interpret this report, consider that a successful "hack" is usually in three parts: (1) identify the vulnerability, the design mistake that permits exploitation; (2) craft the exploit, the computer program that will take advantage of the vulnerability; (3) deploy the exploit. Step 1 might take months or years, and the RAND report describes "stockpiling" identified vulnerabilities. Step 2 takes a median time of 22 days, according to the report. Step 3 is relatively quick. An nonexpert attacker might find or purchase exploits for which steps 1 and 2 have already been done, and simply deploy them; in past decades such attackers were known as "script kiddies".

Even though there are many instances of white-hat hackers demonstrating the insecurity of internet voting systems,[80] ethical hackers are restrained in many ways that malicious hackers are not. Malicious hackers can:

> 1) conduct voter registration attacks, or attacks on authentication systems; 2) circulate malware to infect clients; 3) build spoofing sites and lure mock voters to them; 4) conduct attacks on internet infrastructure, like mail or fax relays, DNS servers, or routers; 5) conduct denial of service attacks; 6) inject malware into software updates that the jurisdiction will install; 7) attack other county or jurisdiction networks as a stepping stone to attacking the election network; 8) attack the vendor's network; 9) bribe or otherwise manipulate officials, jurisdiction employees, or vendor employees; 10) circulate false information to voters; 11) physically burglarize the jurisdiction's premises; 12) loudly proclaim without proof a big lie that they succeeded in rigging the mock election when they did not; 13) take a year or two to prepare, practice, and perfect their attack offline before conducting it for real.[81]

Other considerations restricting ethical hacking of voting systems are discussed by Robinson and Halderman.[82] In summary, even though nobody hacked your system—even when you invited them to—that's not a demonstration of security.

VIII. THE SUBSTANTIVE RIGHT TO VOTE IS NOT FURNISHED BY A VOTING SYSTEM THAT IS HACKABLE SO THAT A SINGLE ACTOR CAN CHANGE VOTES UNDETECTED AT LARGE SCALE

Some people argue, since computers are inherently insecure, let's avoid using them at all to count ballots—let us count paper ballots by hand. That is how votes are counted in many parliamentary democracies such as in Canada, in Europe, and in Australia.[83] In most of those elections, there is only one contest on each ballot.

---

[80] *See generally* Wolchok et al., *supra* note 59; Specter et al., *supra* note 72; Specter & Halderman, *supra* note 75; Springall et al., *supra* note 19; Halderman & Teague, *supra* note 64.

[81] Email from David R. Jefferson, Computer Scientist, Lawrence Livermore Nat'l Lab'y, to author (June 2, 2022, 2:48 pm (PDT)) (on file with author).

[82] *See* David G. Robinson & J. Alex Halderman, *Ethical Issues in E-Voting Security Analysis*, FIN. CRYPTOGRAPHY AND DATA SEC. 119 (George Danezis et al. eds., Springer, Berlin, Heidelberg 2012).

[83] *See e.g., Why Elections Canada Still Uses Paper Voter Lists and Hand Counts Ballots for Federal Elections*, CANADIAN BROADCASTING CORP., https://www.cbc.ca/news/politics/ask-paper-voter-lists-hand-counting-ballots-election-1.6167809 [https://perma.cc/3YTH-WLHE]; *Counting the votes*, AUSTRALIAN ELECTORAL COMMISSION, https://www.aec.gov.au/voting/counting/ [https://perma.cc/FX5N-ECKM]; *See generally Voting in France: Paper Ballots, Cast in Person; no machines*, U.S. NEWS, https://www.usnews.com/news/world/articles/2022-04-08/voting-in-france-paper-ballots-cast-in-person-no-machines [unable to obtain]; *Constitutionality of*

Then it's easy for humans to count votes by sorting ballots into piles and counting each pile.

But the United States has a federal system in which, on the same ballot, there might be dozens or even hundreds of contests. It would be impractical for humans to accurately count those ballots in a timely manner without becoming so tired that they make mistakes. The United States has a long tradition of using mechanical means to count votes.

By now, "mechanical means" means "by computers programmed with software."[84] Computers can count votes extremely accurately—unless they're hacked to be completely fraudulent.[85] Because of this vulnerability to fraud, paperless (touchscreen) voting machines have been largely abandoned by all but a few states.[86]

So: a pure paper-based system without computers is impractical (for U.S. elections), and a pure computer-based system is hackable. The accepted solution, both scientifically and in the states' actual practice, is that voters mark a paper ballot, which is counted by computers (optical-scan voting machines), and which can be recounted or audited by human beings.[87]

Electronic Voting in Germany, NDI, https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany [https://perma.cc/6EH5-XLXJ]; *Guidance for Returning Officers administering Local Government Elections in England*, THE ELECTORAL COMMISSION, https://www.electoralcommission.org.uk/guidance-returning-officers-administering-local-government-elections-england/verification-and-count/count/counting-votes [https://perma.cc/39FA-5KJX].

[84] Since noncomputerized, mechanical lever-action voting machines were banned by the Help America Vote Act of 2002, Help America Vote Act of 2002, Pub. L. No. 107–252, 116 STAT. 1666.

[85] Or unless their sensors/scanners are miscalibrated or clogged with dust. *See* Andrew Appel, *New Hampshire Election Audit, part 1*, FREEDOM TO TINKER (June 2, 2021), https://freedom-to-tinker.com/2021/06/02/new-hampshire-election-audit-part-1/ [https://perma.cc/RKV5-JERJ]; Andrew Appel, *New Hampshire Election Audit, part 2*, FREEDOM-TO- TINKER (JUN. 7, 2021), https://freedom-to-tinker.com/2021/06/07/new-hampshire-election-audit-part-2/ [https://perma.cc/EQB2-E3YN].

[86] *See* The Verifier – Election Day Equipment – November 2024, *supra* note 6 (finding, according to "The Verifier" database maintained by the Verified Voting Foundation, that as of 2022 the only places using paperless DREs were: Louisiana (all parishes); Texas counties representing 4.3% of Texas voters; Indiana counties representing 54% of voters; Tennessee counties representing 40% of voters; New Jersey counties representing 42% of voters).

[87] *See* NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 6–7. ("Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots.").

This "accepted solution" is actually secure ***only if:***

1. Voters mark their paper ballot by hand, not using a machine (a "Ballot Marking Device");[88]
2. When the paper ballots are recounted or audited, it must be by humans looking at them—not by running the ballots again through the same potentially fraudulent computer scanners;[89][90] and
3. Only if the paper ballots *are* actually hand-recounted or hand-audited by a statistically strong method such as a Risk-Limiting Audit (RLA).[91]

Having a paper ballot only offers protection against computer hacking if someone actually looks at the paper! Many states fail on point 1, or point 2, or point 3, or all three.[92] There is much room for improvement. Colorado gets all three

---

[88] *See* Andrew W. Appel et al., *Ballot-Marking Devices Cannot Assure the Will of the Voters*, 19 ELECTION L. J.: RULES, POL., AND POL'Y 432, 432–50 (2020).

[89] *See* NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 94 ("Voter-verifiable paper ballots provide a simple form of such evidence provided that many voters have verified their ballots. The ability of each voter to verify that a paper ballot correctly records his or her choices, before the ballot is cast, means that the collection of cast paper ballots forms a body of evidence that is not subject to manipulation by faulty hardware or software. These cast paper ballots may be recounted after the election or may be selectively examined by hand in a post-election audit. Such an evidence trail is generally preferred over electronic evidence like electronic cast-vote records or ballot images. Electronic evidence can be altered by compromised or faulty hardware or software.")

[90] *See* Andrew W. Appel & Philip B. Stark, *Evidence-Based Elections: Create a Meaningful Paper Trail, then Audit*, 4 Geo. L. Tech. Rev. 523, 538 (2020) (alteration in original) ("The audit must ascertain voter intent manually—directly from the human-readable marks on the paper ballots the voters had the opportunity to verify. It is not adequate to rely on digital images of ballots, printout from an electronic record, barcodes, or other artifacts that are not verifiable by the voter or are not tamper evident. Nor is it adequate to re-tabulate the votes electronically, either from images of the ballots or from the original paper. BMD printouts, digital images of ballots, reprinted ballots, and other computer data are not reliable records of voter intent. They can be incomplete, fabricated, or altered (accidentally or maliciously) by software bugs, procedural lapses, or hacking. Statutes should prohibit relying on such things for the determination of voter intent.").

[91] *See Principles and Best Practices for Post-Election Tabulation Audits*, ElectionAudits.org 1, 14 (2018), https://electionaudits.org/files/Audit%20Principles%20and%20Best%20Practices%202018.pdf [https://perma.cc/RG8E-ZD3J].

[92] The Verified Voting Foundation maintains a database of post-election audit statutes in the 50 states, showing that in most states the audit is not comprehensive (doesn't sample from all the ballots cast), is not binding (if the audit detects the possibility of an incorrect outcome, that does not force a recount), or both.

Overall:

points right,[93] mostly[94], as do Virginia[95] (mostly) and Rhode Island.[96] A few more states are testing pilot RLAs to (eventually) achieve point 3.

But internet voting (electronic ballot return) does not have paper ballots marked by the voter and auditable by human inspection. So this important form of protection (that provides adequate security for hand-marked computer-scanned paper ballots cannot be used) for internet voting.

IX. DIFFERENT FORMS OF INTERNET VOTING HAVE SIMILAR ARCHITECTURES AND SHARE COMMON SOURCES OF INSECURITY

By "internet voting" I mean the return of a voted ballot through the internet from the voter's own[97] computer or smartphone. This could done be by e-mail, by

---

See The Verifier — Post-Election Audits — November 2022, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/audit/year/2022 [https://perma.cc/LW33-TN92].

In which states the result is binding:

See Verified Voting Found., *The Verifier — Post-Election Audits — November 2022*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/binding/year/2022 [https://perma.cc/3UBP-XKJH].

In which states the audit is comprehensive:

See The Verifier — Post-Election Audits — November 2022, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/comp/year/2022 [https://perma.cc/6KSU-7GFQ].

[93] *See* COLO. REV. STAT. § 1-7-515 (2022) ("The general assembly hereby finds … that the auditing of election results is necessary to ensure effective election administration and public confidence in the election process. Further, risk-limiting audits provide a more effective manner of conducting audits than traditional audit methods in that risk-limiting audit methods typically require only limited resources for election races with wide margins of victory while investing greater resources in close races."). *See also* Colo. Code of Reguls., 8 C.C.R. 1505-1 (LEXISNEXIS 2022) (the statute is implemented by rulemaking). The rules make it clear how critically this process relies on having *paper ballots*; so it could not be used for Internet voting.

[94] Colorado's audit system has room for improvement. The risk limit is based on only two contests per jurisdiction; the contests selected are at the discretion of the Secretary of State *after* the results are in, which could permit collusion; the audit could be made more transparent to the public. E-mail from Philip B. Stark, Distinguished Professor, Univ. of Cal., Berkeley, to author (Aug. 10, 2022 02:04 (PDT)) (on file with author).

[95] H.B. 895, Gen. Assemb., Reg. Sess. (Va. 2022).

[96] R.I. GEN. L. § 17-19-37.4 (1956).

[97] In the early 2000s there was also discussion of the "kiosk" form of internet voting, in which the voter would go to a location where a computer owned and managed by election authorities (or a U.S. consulate, or a military base) would be used to create and send the electronic ballot. The kiosk model is not much discussed anymore; it is not what people seem to want. And it suffers

fax, by upload to a web site through a web browser, or by the use of a voting app. Though these may seem like quite different modes, their underlying technology is more similar than different, and they suffer from similar (though not identical) insecurities.

In all of these modes:[98]

1. The voter is authenticated by providing some kind of credential;
2. an unvoted ballot is displayed on a user interface;
3. the voter makes selections in each of the contests;
4. the application (a specialized voting app or simply a browser or PDF web form) displays the selections and allows the voter to review the ballot;
5. the application encodes the voted ballot into a message (perhaps in the form of a PDF file, perhaps not);
6. the application digitally "signs" the message using cryptographic authentication to protect ballots from being altered as they hop from node to node over the internet;
7. the application digitally encrypts the message to protect voters' privacy (the "secret ballot") as the message transits the internet;
8. the voting application (or the voter's e-mail app or browser) transmits the message to election administrators.

The different modes of internet voting handle these individual steps in different ways. Step 1, credentials, is a difficult problem that I will discuss below. Regardless, the critical vulnerability is at step 5. If the voting app (or any layer below it) is hacked—that is, replaced by a fraudulent program under the control of an attacker—it can transmit a *different* ballot than the one that the voter created in step 3 and reviewed in step 4. This is true even if step 5 is performed before step 4. And all of these methods are also vulnerable to server-side attacks, discussed later.

Different internet voting systems implement these steps differently.

E-mail: Some systems allow voters to download a ballot as a PDF file that might look like a standard "fill-in-the-ovals" absentee ballot.[99] The voter fills in the ovals as a "PDF form" using any PDF reader, then e-mails the PDF back to county election officials.[100] This may be particularly unsafe as it may omit steps 5 (digital authentication) and 6 (encryption), making the ballot vulnerable to alteration or inspection as it transits the internet. Even if steps 5 and 6 are not omitted, the ballot

from most, though not all, of the insecurities of other forms of internet voting.

[98] *See infra* Section XVII.

[99] *See* Herrington, *supra* note 33, at 8 fig.3.

[100] *See id.* at 34–35 tbl.5. Those states are AZ, CO, DE, HI, IN, IA, KS, ME, MA, MS, MO, MT, NE, NV, NM, NC, ND, OR, RI, SC, UT, WA, and WV.

is still vulnerable to alteration, *after the voter inspects it*, by a hacked PDF viewer or a hacked operating system.

Fax: Some states allow voting by fax.[101] In the 1980s when fax machines were first in widespread use, the telephone network (on which they operated) was separate from the internet. But now the phone network is just a part of the internet, and most "faxes" are really just uploads to web sites (on the internet) such as HelloFax or Fax.Plus. So voting by fax really is a form of internet voting, with the added vulnerability that the HelloFax servers, if corrupted by hackers or insiders, can alter votes as they transmit ballots.[102]

Upload: Some jurisdictions allow the voter to upload a PDF ballot to a web site.[103] This method suffers from the same critical insecurity at step 5 and from server-side attacks as discussed below.

Special-purpose app: Some systems have a special-purpose voting app that runs on the voter's laptop, tablet computer, or smartphone.[104] This avoids some of the insecurities of unencrypted e-mail or third-party fax servers. Still, in any of these apps there is the critical point between step 4 and step 5 where (if the app is fraudulently hacked) the ballot can be altered.

X. ON THE INTERNET, NOBODY KNOWS YOU'RE A HUMAN: CREDENTIALING THE VOTER IS DIFFICULT

It is a difficult task to determine if an internet message arriving at some server really originated from a specific human being. The general approach to doing this is that the human person knows some secret (such as a password) or possesses an item containing a secret (such as a chip-enabled credit card).[105]

For example, a modern tap-to-pay credit card contains a computer in which there is a secret "signing key" known to no other computer in the world (not even

---

[101] *See id.* at 34–35 tbl.5. Those states are AL, AZ, CA, CO, DE, FL, HI, IN, IA, KS, LA, ME, MA, MI, MO, MT, NE, NV, NM, NC, ND, OK, OR, RI, SC, TX, UT, WA, and WV.

[102] *See* Andrew W. Appel, *Safely Opening PDFs Received by E-mail (or Fax?!)*, FREEDOM TO TINKER (June 24, 2020), https://freedom-to-tinker.com/2020/06/24/safely-opening-pdfs-received-by-e-mail-or-fax/ [https://perma.cc/E3V4-H2BF].

[103] *See* Herrington, *supra* note 33, at 34–35 tbl.5. Those states are AL, AZ, CO, MO, NV, NC, ND, and WV.

[104] *See* Specter & Halderman, *supra* note 75, at 3077–92 (discussing, for example, Democracy Live); *see* Specter et al., *supra* note 72, at 1535–53 (discussing Voatz).

[105] *See* Paul A. Grassi et al., U.S. DEP'T OF COM., NAT'L INST. OF STANDARDS & TECH. SPECIAL PUBL'N 800-63-3 REVISION 3, DIGITAL IDENTITY GUIDELINES (2017), https://pages.nist.gov/800-63-3/sp800-63-3.html [https://perma.cc/7DBJ-AU73] (referencing section 4.3.1).

Visa or Mastercard's server computers).[106] This is an "encapsulated key" system—unlike a Social Security card or driver's license that has the number printed on it that anyone can read. Messages signed by the computer inside the credit card can be authenticated at Visa's servers by doing a mathematical calculation using the "public key" that is the counterpart of the signing key.[107] This gives Visa fairly high assurance, though they still must deal with the problem of physically stolen credit cards.[108]

Estonia issues such a chip-enabled encapsulated-key ID card to every one of its citizens.[109] Estonia also permits internet voting on a large scale.[110] The digital credential may work fairly well, but the Estonian system (like internet voting systems generally) is still vulnerable at the client side (as described above) and the server side (as described below).

Americans do not have such a universal encapsulated-key credential card. Even the new RealID driver's licenses are not encapsulated-key: the QR code is on the outside of the card, where anyone can copy it.[111] And of course, many voters do not have drivers licenses (or nondriver identity cards issued by motor vehicle agencies).

Furthermore, issuing an encapsulated-key voter card to every citizen would not work, if that card could be used only for voting. The Estonian system serves as a useful digital credential because it is used for many everyday purposes, not only voting; so if an Estonian's card is lost, misplaced, or stolen, then they have a real problem and they immediately take steps to report and replace it.[112] In contrast, if

---

[106] Contactless credit cards generally use the EMV protocol, named after the standards organization EMV, emvco.com. These cards support a variety of protocols. In some of these protocols the card's secret key is known both to the card and to Visa or Mastercard's central computer. *See* Joeri de Ruiter, Lessons Learned in the Analysis of the EMV and TLS Security Protocols 14 (Aug. 27, 2015) (Ph.D. thesis, Radboud Universiteit Nijmegen), https://cypherpunk.nl/papers/phdthesis.pdf [https://perma.cc/GR8Z-PWRR] (describing, for example, the "unique symmetric key"). In other EMV protocols in which public-key cryptography is used, it is not necessary for the card's secret key to reside anywhere except on inside the card itself. *See id.* ("Cards that support asymmetric cryptography….").

[107] *See Internet Security Glossary, Version 2*, NETWORK WORKING ROOM 1, 21—22 (August 2007), https://datatracker.ietf.org/doc/html/rfc4949 [https://perma.cc/8JYU-N7LK].

[108] *See* EMVCo L.L.C., *Overview of EMVCo*, EMVCO, https://www.emvco.com/about/overview/ [https://perma.cc/EDV7-MGJA] (last visited July 26, 2022) (providing an overview of the EMV secure payment standards).

[109] *See* Springall et al., *supra* note 19 at 704.

[110] *Id.* at 703.

[111] *See* 6 C.F.R. § 37.19 (2008) (referencing particularly section 37.19, listing the PDF417 standard used for the barcode, and listing the data that must be present there).

[112] *See* EAS Enterprise Estonia, *E-Identity*, E-ESTONIA, https://e-estonia.com/solutions/e-identity/id-card/ [https://perma.cc/B2U4-Q65G].

an American had a voting card used only every two or four years, it is susceptible to undetected misplacement, loss, or theft.

So internet voting systems in the United States have to take other approaches to the voter's digital credentials, such as:

- Send a one-time PIN (for this election only) through U.S. mail to the voter's address of record. This is as approximately secure as sending physical absentee ballot to the voter. It is not perfect, but secure enough and not easily hackable remotely over the internet.
- Send a PIN by electronic means (e-mail or web site), similar to how a blank (unvoted) PDF ballot might be sent to the voter. But how do you know that's really the voter?
- Ask the voter to hold up their driver's license next to their face in front of their computer's or phone's camera.

That last form of human-computer authentication, to associate a particular human person with a particular computer account, came into use in approximately 2010 in private industry.[113] For example, Google used it to authenticate certain kinds of accounts.[114] To serve smaller companies than Google, specialized companies sprang up to provide this kind of authentication as a third-party service.[115]

By 2020, the voting service provider Democracy Live had been contracted by several states to provide internet voting for UOCAVA voters and voters with disabilities.[116] Democracy Live, in order to authenticate the human voter, collected this photo-ID information—in fact,

> In all modes of operation, Democracy Live receives a wealth of sensitive personally identifiable information: voters' names, addresses, dates of birth, physical locations, party affiliations, and partial social security numbers. When ballots are marked or returned online, the company also receives voters' ballot selections, and it collects a browser fingerprint during online voting. This information would be highly valuable for

---

[113] I experienced it myself in approximately 2010 when google asked me to hold my driver's license next to my face and take a selfie, for the purposes of authenticating my Google Scholar account. By now it is ubiquitous: the google search "Confirm your identity with a photo of yourself holding your ID" yields evidence that the following companies and governments use the practice: wise.com, mintra.com, instagram.com, facebook.com, zendesk.com, id.me, tn.gov, edx.org, kraken.com, antarctica.gov.au, mahaguru.de, freelancer.com, passbase.com, cex.io, xfinity.com, yubo.live, clearscore.com, imvu.com, mercuryo.io, turo.com, commsec.com.au, emqsend.com, btseventrentals.com, coventrybuildingsociety.co.uk, and sars.gov.za.

[114] Google's use occurred, in my personal experience, sometime between 2010 and 2015.

[115] For example, ID.me. *See ID.me*, ID.ME, https://www.id.me/ [https://perma.cc/392F-6B9L].

[116] *See* Specter & Halderman, *supra* note 75 at 3079 (referencing section 2.2, Specter and Halderman found evidence of 7 state governments and 98 smaller jurisdictions in 11 states). Of these, 70 offer online ballot marking.

> political purposes or for election interference, as it could be used to target ads or disinformation campaigns based on the voter's fine-grained preferences. Nevertheless, OmniBallot has no posted privacy policy, and it is unclear whether there are any effective legal limitations on the company's use of the data.[117]

This is shocking: it's bad enough that companies like Cambridge Analytica gathered huge amounts of personal information on individual voters for the purposes of microtargeting disinformation—they took that data from people who made the mistake of signing up for Facebook.[118] But for the citizen who just wants to exercise their right to vote, to be forced by the State to surrender personally identifying data to a private company with no apparent restrictions on its use, goes beyond even the Facebook scandal. Consider the backlash in 2022 when the IRS contracted with id.me to provide this same service.[119] No state should participate in such a scheme.

XI. SERVER-SIDE VULNERABILITIES ALSO CAUSE INSECURITY

Once the voter's ballot arrives at the county's election server, it can be counted. But it's not so simple.

First, the server may have been hacked: either by an outsider from the internet exploiting a vulnerability in the server's operating system, by an insider with sufficient access privileges, or by an unprivileged insider who has physical access. It is *extremely* difficult to secure computers against people who have physical access and can open them up with a screwdriver and replace components. If the server is hacked, then fraudulent server-side software can change votes.

Second, many jurisdictions "remake" the ballot to fit into their regular optical-scan voting process.[120] That is, an election worker prints the ballot that was received via the internet from a voter. Then, because a printed PDF ballot may not be exactly the same size and alignment as a preprinted optical scan form, and therefore may scan improperly, the election worker fills in ovals on a preprinted ballot

---

[117] *Id.* at 3078.

[118] Matthew Rosenberg et al., *Firm That Assisted Trump Exploited the Data of Millions,* N.Y. TIMES 1 (Mar. 18, 2018), https://www.nytimes.com/2018/03/17/us/politics/547ambridge-analytica-trump-campaign.html [https://perma.cc/M62P-A8WU].

[119] Alan Rappeport, *IRS Will Allow Taxpayers to Forgo Facial Recognition Amid Blowback*, THE SEATTLE TIMES (Feb. 23, 2022, 8:40 p.m.), https://www.seattletimes.com/nation-world/irs-will-allow-taxpayers-to-forgo-facial-recognition-amid-blowback-2/ [https://perma.cc/TTU6-62GQ].

[120] Michelle Shafer, *Ballot Duplication: What It Is, What It Is Not, and Why We Are Talking About It in 2020*, OVERSEAS VOTING INITIATIVE (JULY 20, 2020), https://ovi.csg.org/ballot-duplication-what-it-is-what-it-is-not-and-why-we-are-talking-about-it-in-2020/ [https://perma.cc/C925-PVZF].

corresponding to what's indicated on the electronically received ballot. In principle, this should be done in front of a witness; and it severely compromises voter privacy, so many jurisdictions make such voters explicitly waive their right to a secret ballot.[121]

Third, in many cases the server is owned and controlled by a private company, such as an election-services provider.[122] Then insiders at the service provider are in a position to change votes without being detected.

Fourth, the server may be "in the cloud." Increasingly, private companies large and small outsource their computing to "cloud computing" providers such as Amazon Web Services, Microsoft Azure, and others.[123] States and counties do so as well.[124] Amazon and Microsoft don't actually have servers in cumulus or cirrus formations in the atmosphere: the racks of computers are on solid earth, where insiders at these private companies have enough access that they could alter many thousands of ballots.[125] Perhaps we trust them, but it is not clear where, in many states, is the authorizing legislation that says that we *do* trust these private companies with the outcomes of our elections.

In fact, it was found that Democracy Live routed ballots and voter information through servers and services provided by Amazon, Google, and Cloudflare: four different private companies handled the same ballot on its way to an election official.[126]

Regarding cloud computing, it is claimed that a service running in the Amazon or Microsoft cloud is secure because Amazon and Microsoft employ "military-grade security."[127] It is certainly true that Amazon and Microsoft employ well designed,

---

[121] Waiving the secret ballot on an individual basis does not actually achieve the purpose for which the secret ballot was introduced 1880-1920, when voter coercion and vote-buying were rampant. Voters can be coerced or bribed into waiving their secret ballot. One of *my* voting rights is that *your* vote was not bought or coerced.

[122] *See* Specter & Halderman, *supra* note 75 at 3078; *see* Specter, *supra* note 72 at 1537.

[123] *See What is Cloud Computing?*, IBM, https://www.ibm.com/topics/cloud-computing [https://perma.cc/ESP6-V8A6].

[124] *The Trusted Cloud for Government*, AWS, https://aws.amazon.com/government-education/government/ [https://perma.cc/5HHM-HXHP] (discussing that Amazon Web Services claims 7500 government agencies).

[125] *See* Edward Moyer, *Ex-Amazon Cloud Worker Found Guilty in Capital One Hack*, CNET (June 18, 2022, 3:08 p.m.), https://www.cnet.com/tech/services-and-software/ex-amazon-cloud-worker-found-guilty-in-capital-one-hack/ [https://perma.cc/Y3FE-3UHW].

[126] *See* Specter & Halderman, *supra* note 75 at 3083, 3088.

[127] *See Voatz Collaborates with WGBH's National Center for Accessible Media to Make Mobile Voting Accessible for Voters with Disabilities and Citizens Residing Overseas*, VOATZ (Nov. 4, 2019), https://voatz.com/category/press/page/2/ [https://perma.cc/45PF-KSQQ] ("Voatz is an

sophisticated, state-of-the-art security mechanisms.[128] But even so, their systems may have vulnerabilities. More to the point, what Amazon and Microsoft provide is a *virtual machine platform* on which customers (such as Democracy Live or a state or county) run the operating system and application of their choice.[129] Insecurities in those layers are the same as if they were running on a local server and are beyond Amazon's or Microsoft's control. The term "military grade security" (as I have seen it used in describing voting systems) is just advertising puffery.[130]

XII. WHAT IS AND WHAT IS NOT A "PAPER TRAIL"

Paper ballots have a useful kind of "paper trail:" the voter marks a sheet of paper; the election administrator counts that same sheet of paper, first by machine and perhaps later by hand.

Some internet voting vendors falsely claim to have a paper trail.[131] In their systems, the voter e-mails or uploads an electronic ballot to a county election official who prints it out onto paper and then counts it in the regular optical-scan vote counters along with other ballots marked directly by voters.[132] Look, the vendors of these systems say, there is a paper ballot![133]

But this is a sham. The voter never gets to see this paper and cannot verify that the correct votes are recorded on it.[134] If the ballot has been altered in the process of

---

award-winning mobile elections platform that leverages military-grade technology … to increase accessibility and security in elections").

128 These qualities are based on my experience over many years speaking with computer scientists and technologists from Amazon and from Microsoft.

129 *See Amazon EC2*, AWS, https://aws.amazon.com/ec2/ [https://perma.cc/UV4A-L8BX].

130 Many companies (not only voting-system vendors) advertise their products with the term "military-grade security" or "military-grade encryption." By this they seem to mean that they have used (as one component of a large system) some encryption algorithm such as AES that the military also uses, or that might have been originally specified in the context of a military applications. But highly secure systems do not achieve security (when they manage to achieve it) simply by tacking on the use of an encryption algorithm; it requires top-to-bottom attention and review. There are some military systems in which this attention has been paid; but this has little to do with the use of the term in commercial advertising of nonmilitary products.

131 *See* Democracy Live, Inc., *OmniBallot Fact Sheet*, DEMOCRACY LIVE (Mar. 20, 2020), https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf [https://perma.cc/N4X5-F7FX] (making the false claim that "OmniBallot is not an online voting system.").

132 *Id.*

133 *Id.*

134 *Id.*

being electronically packaged for transmittal over the internet, nobody will be able to notice the change.

XIII. SAFE USES OF THE INTERNET IN CONNECTION WITH VOTING

It is reasonably safe to do a banking transaction by internet because there is end-to-end per-transaction auditability —that is, you can review your bank statement and see the transaction, verify that the amount is correct, and notice whether the bank lists any transactions you don't recognize. And if your computer has been so hacked that your online-banking app starts misrepresenting these to you, you'll eventually notice when your credit card is declined or your checks bounce. You can also contact the bank by other means (e.g., telephone) to check on transactions and balances, and banks can confirm transactions through other channels such as text messages.

There is nothing analogous in voting because of the secret ballot. You can't call up an election official (or go online) to ask, "can you confirm that I voted for Smith?" You will have no way of knowing whether your vote was counted correctly. This is a key difference between banking and voting: ability/inability of the user to do per-transaction auditing.

But some things connected to elections *do* have per-transaction user-auditability.[135] If you register online to vote, you can call the county superintendent of elections to confirm that you're registered; or you'll find out one way or another when you try to vote or check the on-line web site. If your voter registration is hacked, you will eventually notice. This basic fact helps to make online voter registration adequately secure.

The same is true for online transmission of an unvoted PDF-file ballot from an election administrator to a voter. Many states have such systems for UOCAVA voters. The voter is expected to print the unvoted absentee ballot, fill in the ovals, and return it by (physical) mail. This is secure enough. And it helps address the problem of slow overseas mail systems since paper needs to be mailed only in one direction instead of round-trip.

Physical return of voter-printed PDF ballots still poses problems for election officials: the paper ballot will likely need to be "remade" for the reasons described above. Remaking is labor-intensive and error-prone, so election administrators have good reason to limit it to those voters specifically in need: such as those abroad or with disabilities.

---

[135] Examples are given in the next two sentences.

XIV. LAWSUITS AND LEGISLATION

In the twentieth century, voters with disabilities that prevented them from operating a lever voting machine, a punch-card voting system, or a hand-marked paper ballot required the assistance of another person in order to vote.[136] Most states allowed (and still allow) a disabled voter to bring a person of their choice to the polls to mark a ballot for them; can ask a poll worker to mark the ballot for them; or can vote absentee, with the assistance of another person at home.[137]

By the turn of the century, computer-based interfaces held the promise of providing assistive technology that could allow persons with visual disabilities or motor disabilities to vote *independently,* without the assistance (and the privacy invasion) of another person.[138] Computer touchscreens could serve persons with reduced vision by magnifying the names on the ballot. Audio interfaces (with headphone jacks) could read the ballot to a blind voter and allow navigation via buttons. Sip-and-puff input devices could accommodate voters with quadriplegia.

Also by the turn of the century, after the debacle in the *Bush v. Gore* election in Florida with punch-card ballots (punch cards are a truly bad voting technology for several reasons), it was clear that many states would have to replace their voting systems, and it seemed that computerized voting machines were the solution.

Of course, by 2000 more than half the states did already use a computerized voting technology that was, and is, reliable, accurate, and secure:[139] hand-marked optical scan ballots, counted by computers (optical-scan voting machines), and recountable by hand.

Still, by 2002 it seemed to the U.S. Congress that paperless touchscreen (or

---

[136] *See* DOUGLAS W. JONES & BARBARA SIMONS, BROKEN BALLOTS: WILL YOUR VOTE COUNT? 221 (CSLI Publ'ns 2012) (discussing, in section 9.3, "a 1982 amendment to the *Voting Rights Act* (VRA) of 1965 contains a provision allowing voters with disabilities to bring someone to assist them at the polls."). *See* H.R. 3112, 97th Cong. § 208, 96 Stat. 135 (1982) (enacted).

[137] In particular, it's been Federal Law since 1982. *See id.*

[138] *See generally* JONES & SIMONS, *supra* note 136 at ch. 9 (CSLI Publ'ns 2012) (describing early 21st century voting machines that used these technologies).

[139] Optical-scan voting systems *can* be secure, if proper chain-of-custody measures are taken for the ballots, risk-limiting audits (RLAs) actually do examine the paper ballots after the election, the ballots are designed correctly, and the machines are properly maintained. *See* Appel & Stark, *supra* note 93 at 523-41; *see* Andrew Appel, *Florida Is the Florida of Ballot-Design Mistakes*, FREEDOM TO TINKER (Nov. 14, 2018), https://freedom-to-tinker.com/2018/11/14/florida-is-the-florida-of-ballot-design-mistakes/ [https://perma.cc/9BSP-9K4H]; *see also* Appel, *supra* note 88 (finding optical scan *can* be reliable, but not if the machines are ill-maintained and the ballots are improperly folded). Optical-scan voting systems are the least insecure, least unreliable, least inaccurate method of voting that I know of; but security, reliability, and accuracy still take effort to achieve.

screen and buttons) computer-based voting machines could solve two problems at once: replacing the inaccurate punch-card systems and providing an accessibility solution for voters with disabilities.[140] These machines, called *direct-recording electronic* (DRE) voting machines, were newly on the market. The Help America Vote Act of 2002 outlawed mechanical lever machines and punch-card voting; provided millions of dollars to assist the states in replacing those machines; and required the availability of an "accessible" voting machine in every polling place.[141] Many jurisdictions responded by adopting DREs.[142] Some other states and counties adopted (or continued to use) optical-scan systems with hand-marked paper ballots but provided a DRE for disabled voters.[143] Other jurisdictions used optical-scan systems but provided a *ballot marking device* (BMD): a computer-based system with touchscreen (for voters with moderate vision or motor disabilities), an audio interface (for voters with severe vision impairment), and sip-and-puff.[144] After the voter prepares the ballot on the BMD, the BMD prints an optical-scan paper ballot that can be scanned by the same voting machines that accept hand-marked ballots.[145]

After 2002 almost a third of the states adopted DREs for all or most voters.[146] But by 2004, computer scientists were pointing out that they are hopelessly insecure: if the computer is hacked to alter votes, there's no paper trail that can correct them.[147] And by 2008 all but two or three states had realized this: after 2008

---

[140] *See* Help America Vote Act of 2002 (HAVA), Pub. L. No. 107-252, 116 Stat. 1666 (West) (codified as amended in scattered sections of 52 U.S.C.A.) (explaining that these assumptions are behind the accessibility provisions of the 2002 HAVA act).

[141] *See id.* codified as amended in scattered sections of 52 U.S.C.A.).

[142] *See The Verifier — Accessible Equipment — November 2006*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/accEquip/mapType/normal/year/2006 [https://perma.cc/J2GG-LHDX].

[143] *Id.*

[144] *Id.*

[145] *See* NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 39.

[146] *See The Verifier — Election Day Equipment — November 2006*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2006 [https://perma.cc/BBE9-WZ3V].

[147] Sam Lubell, *To Register Doubts, Press Here*, N.Y. TIMES (May. 15, 2003), https://www.nytimes.com/2003/05/15/technology/to-register-doubts-press-here.html [https://perma.cc/G37F-UJCK]

("A group of more than 100 technologists, led by David Dill, a professor of computer science at Stanford University, has called for tighter security measures on electronic voting apparatus and a 'voter-verifiable audit trail,' meaning a permanent record of each vote that can be checked for accuracy even after the election.

no state switched from another technology to paperless DREs; and by 2014 only ten states and by 2020 only six states were still using them.[148] By 2022 it was only Louisiana and some counties in five other states.[149] Most states use paper ballots, marked by hand or by BMD, that are scanned by optical scanners.[150]

But this has also meant that voters with disabilities were left without DREs as a usable accessible means of voting independently. In fact, DREs never worked well as an accessible technology.[151] In principle it ought to be possible to design a DRE that's truly accessible, but the ones actually purchased and deployed had terrible user interface designs.[152] Furthermore, since a typical polling place might have only zero or one voter arrive who wanted to use the accessibility feature, poll workers were poorly trained in setting them up.[153] Once DREs were abandoned for nondisabled voters (in favor of optical-scan), there was the additional problem that the (one or two) DRE-recorded votes were counted separately from the others, so

---

. . . Without such a trail, Dr. Dill warned, if a machine is tampered with or malfunctions, 'then the votes in question are corrupted and you have no option but to hold another election or accept bad results.'").

148 "Four or five" is an approximation reflecting the fact that in many states the choice of voting machines is left up to each county. *See The Verifier — Election Day Equipment — November 2008*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2008 [https://perma.cc/762H-EYC3]; *see The Verifier — Election Day Equipment — November 2014*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2014 [https://perma.cc/L9VW-WCDW]; *see The Verifier — Election Day Equipment — November 2020*, THE VERIFIER, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020 [https://perma.cc/7NLC-NLWP].

149 *Id.*

150 *Id.*

151 *See* Andrew Appel, *Accommodating Voters with Disabilities*, FREEDOM TO TINKER (May 27, 2021), https://freedom-to-tinker.com/2021/05/27/accommodating-voters-with-disabilities/ [https://perma.cc/VR4Y-KQLQ].

152 This statement is based on several experience reports from Noel Runyan, a California computer scientist who is blind. Mr. Runyan in at least 17 elections between 2004 and 2016 used the supposedly "accessible" interface on various voting machines (over the years) at his local polling place, and documented how these machines were barely usable at all by blind voters. Email from Noel Runyan to author (Nov. 10, 2008) (on file with author); Email from Noel Runyan to author (Nov. 16, 2016) (on file with author); Email from Noel Runyan to author (June 7, 2018) (on file with author) [hereinafter *Emails from Noel Runyan*]. *See also* JONES & SIMONS, *supra* note 136 at 215–17.

153 Emails from Noel Runyan, *supra* note 152.

voters with disabilities effectively lost the secret ballot.

Disability-rights activists pushed election officials to deploy solutions such as,

- Better train poll workers in the rights of disabled voters and in the means of accommodating them;[154]
- Make polling places more (wheelchair) accessible and make election websites more accessible to blind voters (by avoiding web-page designs that accessibility-enabled browsers can't interpret);[155]
- Provide accessible BMDs; but this has the disadvantage that a voter must still handle the paper ballot, which is difficult or impossible for some voters;[156]
- Provide "curbside voting," in which an election worker brings a portable (BMD or DRE) voting machine to the voter (in their car or in their home);[157]
- And finally, provide "Remote Accessible Vote By Mail" (RAVBM), which might or might not mean some sort of internet voting system.[158]

In 2020, there were lawsuits in at least five states in which disability-rights plaintiffs demanded that election officials implement one or more of these measures.[159] In many of those states, election-security advocates pushed back on any form of *electronic ballot return*—that is, any version of RAVBM in which voted ballots were transmitted over the internet from the voter's computer or phone.[160]

---

[154] *See* Acro Media, Inc., *Training the Poll Worker: Empowering the Blind Voter,* NAT'L FED'N OF THE BLIND, https://nfb.org/programs-services/center-excellence-nonvisual-access/national-center-nonvisual-election-5 [https://perma.cc/RU6V-ZGTC].

[155] For example, in 2016 the National Federation of the Blind and the Center for Independent of the Disabled sued New York; the lawsuit was settled after 34 days with the State Board of Elections and the Department of Motor Vehicles agreeing to make certain changes to their website. *See* Stipulation on Plaintiffs' Motion for Preliminary Injunction, Eason v. N.Y. State Bd. of Elections, No. 1:16-cv-04292-KBF (S.D.N.Y. Aug. 11, 2016), https://bzd3bc.a2cdn1.secureserver.net/wp-content/uploads/2016/09/9-8-16-New-York-Online-Voting-Stipulation.pdf [https://perma.cc/F5TK-3KUK].

[156] *See* Press Release, National Disability Rights Network, *Disability Community Fears Paper Ballot Mandate Will Hurt Voters with Disabilities* (January 29, 2021) (https://www.ndrn.org/resource/disability-community-fears-paper-ballot-mandate-will-hurt-voters-with-disabilities/ [https://perma.cc/K2ER-Z8NT]).

[157] *Curbside Voting*, NORTH CAROLINA STATE BOARD OF ELECTIONS, https://www.ncsbe.gov/voting/help-voters-disabilities/accessible-voting-sites/curbside-voting [https://perma.cc/L5X2-UDWA].

[158] *See supra* Section III.

[159] *See infra* Section XV.

[160] *See id.*

The other accommodations are clearly a good thing (better training, accessible Polling places and web sites,[161] accessible BMDs, curbside voting, and other forms of RAVBM), and these were not opposed by election-security advocates.

XV. FIVE 2020 LAWSUITS DEMANDING RAVBM

In 2020, the National Federation of the Blind sued the State of **Virginia** asking for remote accessible vote-by-mail (RAVBM) including "electronic delivery and marking of absentee ballots."[162] In such a system, the voter uses their own home computer to download an unmarked absentee ballot and then has two options: (1) print it out and fill in the ovals by hand, as they would a preprinted absentee ballot, or (2) use a software application to indicate their choices, which then prints out a marked ballot with the ovals filled in.[163] Option 2, "electronic marking of absentee ballots," can be useful to voters with disabilities, who have the assistive technology of their choice already installed on their own computer.[164] But it has a security risk: if the voter's computer has been penetrated by attackers, the votes on the paper ballot could be different than what the voter indicated. This risk is (perhaps) acceptably mitigated by the end-to-end paper trail: the very same sheet of paper with votes marked on it, which the voter can inspect after printing, is the one counted by optical-scan voting machine and recountable by human eyes.[165] This security mitigation—the voter's own inspection of the paper ballot—still poses difficulties for blind voters, but not necessarily insurmountable ones: many people with severe visual impairment possess text-reading devices to read aloud what is printed on paper.[166]

---

[161] I note with concern, however, that supposedly "accessible web sites" may not actually be usable by blind voters. *See* Amanda Morris, *For Blind Internet Users, the Fix Can Be Worse Than the Flaws*, N.Y. TIMES (July 13, 2022), https://www.nytimes.com/2022/07/13/technology/ai-web-accessibility.html [https://perma.cc/59UV-7PJ5].

[162] Opinion on Plaintiff's Motion for Preliminary Injunction, Gary v. Va. Dep't of Elections, No. 1:20-CV-860, 2020 U.S. Dist. LEXIS 214886, at *1 (E.D. Va. Aug. 28, 2020).

[163] *See supra* Section III.

[164] *See id.*

[165] Except for the issue of "remaking" which can introduce errors or insecurities but is, at least, performed by human election officials who are (in principle) not subject to large-scale remote hacks. *See* Shafer, *supra* note 120 (discussing the issue of "remaking").

[166] Unfortunately, however, those paper-scanning tools do not generally cope well with the format of an optical-scan ballot. According to Noel Runyan, a computer scientist and voting-system expert who is legally blind (*See supra* note 152), more work is needed in "Development of scanning apps for accessible verification of paper ballots with ballot mark-sensing optical character recognition (OCR)." *See* Appel, *supra* note 151.

The RAVBM system requested by the Virginia Plaintiffs did *not* include electronic ballot return (internet voting).[167] According to the scientific consensus, an RAVBM system such as Plaintiffs requested is not considered unacceptably insecure.[168]

Within seventeen days, the parties settled[169] for a system generally similar to the requested relief.

In 2020, the New Jersey Division of Elections (within the office of Secretary of State) quietly took steps to allow internet voting; and subsequently were sued on the basis that this would be both insecure and illegal; and agreed not to pursue internet voting in New Jersey, but to use other means to accommodate voters with disabilities (citation and discussion below).[170]

In 2020, a group of plaintiffs living abroad sued New York and six other states in U.S. District Court asking for internet voting.[171] Within four days of Plaintiffs' motion for a preliminary injunction, motions in opposition had been filed by Ohio, Texas, Kentucky, Wisconsin, New York, Georgia, and Pennsylvania; accompanied by fourteen declarations from election security experts, organizations representing UOCAVA voters, state election officials, and others.[172] Defendants pointed out (1)

---

[167] *See* Gary v. Va. Dep't of Elections, No. 1:20-CV-860, 2020 U.S. Dist. LEXIS 214886, at *2—3 (E.D. Va. Aug. 28, 2020).

[168] This consensus study report from the National Academies of Science, Engineering, and Medicine mentions at-home electronic ballot marking without comment on its security or insecurity: "Some states accommodate remote accessible ballot marking. In such states, a voter retrieves and marks a ballot online, prints out the completed ballot, and mails the ballot to the appropriate election's office." *See* NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 39. The report discusses electronic transmission of unmarked ballots to voters, but regarding its security simply says, "However, it appears that no peer-reviewed research has comprehensively assessed the relative risk-reward tradeoffs involved in using the mails to transmit absentee ballot requests and unmarked ballots." *See id.* at 94.

[169] *Gary,* 2020 U.S. Dist. LEXIS 214886, at *1.

[170] *See generally* Gusciora v. McGreevey, 929 A.2d 599, 599 ((N.J. Super. Ct. App. Div. 2006)); , rev'd sub nom. Gusciora v. Corzine, No. MER-L-2691-04, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *1 (Feb. 1, 2010); Gusciora v. Christie, No. A-5608-10T3, 2013 N.J. Super. Ct. App. Div. LEXIS 2278, at *1 (Sept. 16, 2013).

[171] *See generally* Harley v. Kosinski, No. 1:20-cv-04664, slip op. (E.D.N.Y. Apr. 9, 2021).

[172] *See generally* Memorandum in Support of Motion to Dismiss, in Opposition to Motion for Preliminary Injunction, and in Support of Motion to Sever and Transfer, *Harley*, slip op.; New York State Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction, *Harley*, slip op.; The Pennsylvania Defendants' Memorandum of Law in Opposition to the Plaintiffs' Motion for a Preliminary Injunction, *Harley*, slip op.; Brief of Wisconsin Elections Commissioners in Opposition to Preliminary Injunction, *Harley*, slip op.; Defendant Ohio Secretary of State Frank Larose's Memorandum in Opposition to Plaintiffs' Motion for

the insecurity of voting by internet, (2) the difficulty of implementing such changes less than a month before the November 2020 election, and (3) reasonable accommodations already in place for UOCAVA and disabled voters.[173] The court denied a preliminary injunction, and then Plaintiffs moved to dismiss the case.[174]

In 2020, the National Federation for the Blind sued **New Hampshire** asking for internet voting and for accessibility improvements in the State's election website (that provides information for voters).[175] The parties settled for no internet voting, for other accommodations for voters with disabilities (some of which New Hampshire already had in place), and for improvements in the web site.[176]

In 2020, the North Carolina Council for the Blind sued the **North Carolina** State Board of Elections, demanding that the Board offer "alternative format absentee ballots allowing private and independent method of absentee ballots that is accessible for Plaintiffs and others with vision disabilities.[177]" The eventual court order required RAVBM with electronic ballot return at least for the 2020 election, and the case was settled in August 2021.[178]

I will discuss the New Jersey and the North Carolina cases in more detail. In New Jersey, a lawsuit[179] filed in 2004 sought to enjoin the use of DREs on state-constitutional grounds (that the substantive right to vote requires reasonably securely counting those votes). It went to trial in 2009.[180] The Court's 2010 ruling did not ban DREs, but the court did order that voting systems must not be

---

Preliminary Injunction, *Harley*, slip op.

173 *See generally id.*

174 *See generally id.*, (order denying preliminary injunction) [but also this: NOTICE OF VOLUNTARY DISMISSAL PURSUANT TO F.R.C.P. 41(a)(1)(A)(i). Pursuant to F.R.C.P. 41(a)(1)(A)(i) of the Federal Rules of Civil Procedure after conferring with Defendants as suggested by the Court, the Plaintiffs and their counsel hereby give notice that the above-captioned action is voluntarily dismissed, without prejudice against all Defendants. Date: October 13, 2020].

175 Frye v. Gardner, No. 20-cv-00751-SM. 2020 U.S. Dist. LEXIS 230785, at *1 (D. N.H. Dec. 9, 2020).

176 *See generally id.*

177 Complaint at 23, Taliaferro v. N. Carolina State Bd. of Elections, 489 F. Supp. 3d 433 (E.D.N.C. 2020).

178 *Taliaferro*, 489 F. Supp. 3d at 440.

179 *See* Gusciora v. McGreevey, 929 A.2d 599, 599 ((N.J. Super. Ct. App. Div. 2006)); , rev'd sub nom. Gusciora v. Corzine, No. MER-L-2691-04, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *1 (Feb. 1, 2010); Gusciora v. Christie, No. A-5608-10T3, 2013 N.J. Super. Ct. App. Div. LEXIS 2278, at *1 (Sept. 16, 2013).

180 *Gusciora*, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *18.

connected to the internet.[181] In March 2020 the New Jersey Division of Elections contracted with Democracy Live to provide an accessible RAVBM solution that included electronic ballot return.[182] On the basis of the 2010 Order[183] that continues in effect, the same plaintiffs filed in April 2020 an emergency motion to enjoin electronic ballot return. The Court ordered plaintiffs and State defendants to engage in settlement talks.[184] The case settled[185] on June 19, 2020: The State agreed to abandon the Democracy Live system and adopted a system from VotingWorks that does not include electronic ballot return.[186]

In the North Carolina case,[187] the plaintiffs did not specifically demand internet ballot return. Instead, they demanded compliance with the Americans for Disabilities Act that requires "reasonable modifications in the Absentee Voting Program to avoid discrimination against Plaintiffs on the basis of disability.[188]" The Plaintiffs also explained methods that other states were already using to accomplish this [all excerpted verbatim from the Complaint[189]]:

- Maryland developed an online marking tool that allows voters to access and mark their absentee ballots on their computers. . . . Although the absentee ballot must still be printed, signed, and returned to the voter's local board of election, voters need not sacrifice the secrecy of their ballots to receive assistance with signing because the signature page prints separately from the ballot.[190]
- Oregon, Wisconsin, and New Hampshire have employed an accessible electronic voting system that can be used for both in-person and absentee voting.[191] Using the platform, voters can access their absentee

---

181 *Id.* at *353.

182 *Id.*

183 *Id.*

184 *Id.* at *346—54.

185 Memorandum of Understanding, Gusciora v. Corzine, No. MER-L-2691-04, 2010 N.J. Super. Ct. Law. Div. LEXIS 2319, at *1 (Feb. 1, 2010);

186 E-mail from Susan M. Scott, Deputy Attorney General of New Jersey, to Penny Venetis (attorney for Plaintiffs), dated June 9, 2020: winning vendor to the State's Bid #20-DOS-528 for an electronic ballot access and delivery system for the July 7, 2020 election is Voting Works with their "VotingWorks Accessible VBM" system.

187 Taliaferro v. North Carolina State Bd. of Elections, 489 F. Supp.3d 433, 435 (E.D. N.C. 2020).

188 Complaint at 19, *Taliaferro,* 489 F. Supp.3d 433.

189 *See id.* at 12—15.

190 *Id.* at 12.

191 *Id.* at 13.

ballots through their web browser and mark their ballots on their computers.[192] Voters then print their ballots and mail them back to their local boards of election where their votes are counted.[193]

- West Virginia has similarly provided an electronic absentee ballot delivery and marking tool to voters with disabilities.[194] Voters access the electronic absentee ballot tool via a web portal, where they are guided with on-screen instructions on how to open and complete the electronic ballot.[195] After completing the ballot, West Virginia law provides that qualifying voters may either (1) print and mail their absentee ballot to their county clerk or (2) submit their absentee ballot electronically to their county clerk directly through the web portal.[196]
- Alaska [has] provided accessible remote voting options for some elections . . . an electronic absentee ballot that can be completed and transmitted using the voter's computer.[197]
- Michigan made its UOCAVA PDF ballots accessible and available to blind voters . . . [but no electronic return of voted ballots].[198]
- New York . . . agreed to email accessible absentee ballots to qualified voters with disabilities [but no electronic return of voted ballots].[199]

The Complaint explained this variety of ways in which other states had complied with the ADA but did not specifically request internet ballot return.[200] The motion for preliminary injunction was similarly open-ended.[201] Only two of the eight states referred to in the Complaint permitted electronic ballot return as a disability accommodation.[202]

At that time, North Carolina was already adopting Democracy Live's system to

---

192 *Id.*

193 *Id.*

194 *Id.*

195 *Id.*

196 *Id.*

197 *Id.* at 14.

198 *Id.*

199 *Id.* at 15.

200 *Id.*

201 *See generally* Motion for Preliminary Injunction, *Taliaferro*, 489 F. Supp.3d 433.

202 As is clear from the *Complaint* itself in paragraphs 45-48. Complaint at 12—14, *Taliaferro,* 489 F. Supp.3d 433.

accommodate UOCAVA voters (i.e. voters living abroad).[203] The final settlement accepted by the Court in August 2021 called for the use of that system, including RAVBM with electronic ballot return to accommodate voters with disabilities.[204]

In effect, the plaintiffs, by failing to request a specific remedy, dumped the problem onto the Court to devise a solution. The Court reached for the most convenient solution to get the case off its docket. The result is that North Carolina voters with disabilities, unlike those in most states, are subjected to the insecurity of internet ballot return.[205] This is perhaps not the best way to make public policy.

XVI. NEW JERSEY'S UOCAVA VOTING SYSTEM: A PAPER TRAIL

Like many states, New Jersey allows UOCAVA voters to download an unvoted ballot in PDF format, print it, mark it, and return it.[206] As in several other states, the voter may return the marked ballot either by physical mail or electronic means.[207] Unlike in other states, if the voter returns the marked ballot electronically—by scanning it and e-mailing the image—that voter must also airmail the physical ballot to the county election administrator.[208] The vote can be *counted* as soon as it arrives electronically, even before the paper ballot arrives.[209]

The purpose is to protect against hacked computers altering the ballot without detection—either the voter's computer or the county election clerk's computer. The voter marks a piece of paper, and the election clerk reads the same piece of paper; no computer hack can intervene. And then:

> Prior to certification of the results of the election, the county board shall: (1) compare the information on the copy transmitted by electronic means … with the … ballot sent by air mail … (2) ascertain whether an original voted ballot has been received for each copy of a voted ballot received by electronic means and counted. Whenever the … voted ballot transmitted by electronic means [does not match the] ballot sent by air mail … those ballots and all other pertinent documents and information relative to those ballots shall be turned over to the superintendent of elections [or] prosecutor for further

---

[203] According to the Internet Archive, as of October 1, 2020, the "North Carolina Absentee Ballot Portal" at https://votebymail.ncsbe.gov/app/home stated at the bottom, "Powered by Democracy Live". *See* North Carolina Absentee Ballet Portal, NORTH CAROLINA STATE BOARD OF ELECTIONS, https://votebymail.ncsbe.gov/sites/37/app/home [https://web.archive.org/web/20201001170927/https://votebymail.ncsbe.gov/app/home].

[204] *Taliaferro,* 489 F. Supp.3d at *440.

[205] *Id.*

[206] N.J. STAT. ANN. § 19:59-14 (2022).

[207] *Id.*

[208] *Id.*

[209] N.J. STAT. ANN. § 19:59-15 (2022).

investigation and action.[210]

I suspect that many UOCAVA voters do not, in practice, mail that paper ballot as they are supposed to; and I suspect that many county election officials do not report or do not take action as required by law when that happens. The statute does not specify what that "action" should be. The law requiring paper-ballot airmail follow-up may be "security theater."[211]

XVII. END-TO-END VERIFIABLE INTERNET VOTING: PERHAPS SOMEDAY THIS CONCEPT WILL BE SECURABLE IF SCIENTIFIC BREAKTHROUGHS ARE ACHIEVED

The central problem that makes internet voting so hard to secure is that the secret ballot interferes with individual-transaction auditability. If we didn't need the secret ballot, then we could have secure "virtual-bulletin-board" internet voting. In such a system, voters would transmit their ballot (with their name attached), and election officials would post every ballot (with name attached) on a public electronic bulletin board. Voters could look up their ballots to make sure they are listed correctly. Of course, if the voter's computer is hacked enough to alter the ballot on the way out, the same hack could also misrepresent the bulletin board back to the voter; but you could work around that problem: you could inspect the bulletin board using a different computer, or you could ask the person who coerced or bought your vote to check it for you.

But we do have, and we do need, the secret ballot as protection against voter coercion and vote-buying. So, in the late twentieth century some computer scientists devised an ingenious cryptographic protocol that preserves the secret ballot but allows, almost, looking up your individual vote.[212] I lack room here to explain all the details, but in summary, imagine this: First you flip a coin and don't tell your computer whether it's heads or tails. If heads, you prepare and transmit your vote (and perhaps it is hacked in the process; you don't know). If tails, you prepare and transmit a vote that's not necessarily how you really want to vote. Then, if heads, you inform the authorities to count your vote; and if tails, you inform the authorities to reveal *and discard* your vote. If the computer is cheating, you have a

---

[210] *Id.*

[211] Security theater is the practice of taking security measures that are intended to provide the feeling of improved security while doing little or nothing to achieve it. *See* Laura Fitzgibbons, *Security Theater*, TECHTARGET (Apr. 2019), https://www.techtarget.com/whatis/definition/security-theater [https://perma.cc/PUM3-APJA].

[212] Josh Benaloh & Dwight Tuinstra, *Receipt-Free Secret-Ballot Elections (Extended Abstract)*, PROCEEDINGS OF THE TWENTY-SIXTH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING, 544, 548 (1994).

chance of catching it (tails). Or (heads) your ballot is kept secret, but you can't catch it cheating. On the average, any systematic cheating will be caught.

This is a form of *End-to-End Verifiable Internet Voting (E2E-VIV).* There are other forms of E2E-VIV; too complicated to describe here. They are based on scientific principles.

But all known forms of E2E-VIV have at least two severe problems:

1. They lack a *dispute resolution procedure.* That is, a voter may be able to detect that a vote has been altered but has no way to prove that to election authorities.[213] Therefore it's not clear what election authorities should do to correct the election.
2. They require participation from voters in a nonintuitive protocol that is difficult to trust without understanding the underlying mathematics.[214]

To use a technical term, E2E-VIV is Not Ready for Prime Time. Perhaps some usable form will be invented in the future. Decades after the original scientific proposals for E2E-VIV, this hasn't happened yet.

XVIII. SWITZERLAND: CASE STUDY OF A TECHNOLOGY AND HOW TO RESPONSIBLY ASSESS IT

The experts wrote in 2018, "no known technology" can make internet voting secure.[215] In 2019 Switzerland was deploying internet voting with a new technology.[216] The experts ought to take this seriously and not dismiss it out of hand. They did take it seriously, and there are some lessons from what happened next. In short: it's an interesting technology; assessing new technologies is not cheap and easy; and when the new technology *was* finally assessed in depth, the Swiss government decided to put the whole idea on pause.[217]

In 2000 the Swiss Parliament directed the Federal Chancellery to study the feasibility of internet voting.[218] Based on those studies, several cantons

---

[213] David Basin et al., *Dispute Resolution in Voting*, ARXIV (May 28, 2020), https://doi.org/10.48550/arxiv.2005.03749 [https://perma.cc/SN59-BWG5].

[214] *Id.* ("[T]he effective wide-scale deployment of E2E-verifiability will require a broad understanding of the underlying cryptographic methods by election officials and the general public.").

[215] *Id.* at 106.

[216] Haines et al., *supra* note 69 at 644.

[217] *See id.*

[218] *See generally* Jan Gerlach & Urs Glasser, *Three Case Studies from Switzerland: E-Voting,* BERKMAN CTR. FOR INTERNET & SOC'Y HARVARD UNIV. 1 (Mar. 2009), https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-

experimented with pilots starting about 2004.[219] In 2019 the Swiss Post (the national post office) deployed a new system descended from a system originally developed by Scytl.com.[220] The Swiss Post internet voting system was supposed to solve both the server-side security problem (i.e., to prevent hacked servers from stealing votes) and the client-side security problem (i.e., to prevent a hack of the voter's computer from being able to steal votes).[221]

On the server side, the Swiss Post system uses cryptographic "mixnets," a decades-old scientific idea for e-voting[222] that allows servers to count votes while preserving the secret ballot (no server can trace a ballot back to a specific voter). On the client side, the system relies on a sheet of paper sent to the voter that contains secret codes the voter can see, *but the voter's computer cannot see*.[223] Even if the voter's computer is hacked, the hack cannot change votes without knowing those secrets.

This is not a purely paperless internet voting system. It has electronic ballot return, but it relies critically for its security on sending a sheet of paper through the mail from the election office to the voter; this cannot be done by e-mail, otherwise the (possibly hacked) voter's computer will learn the secret codes.

Soon after the system was announced, four scientists (from Norway, Canada, Belgium, and Australia) published a paper[224] showing that the cryptographic design of the Swiss Post mixnet was flawed, allowing opportunities for undetectable fraud. Soon after that, in July 2019, Swiss Post ceased offering its system to the cantons.[225] The Federal Chancellery was commissioned to work with the cantons to

---

Gasser_SwissCases_Evoting.pdf [https://perma.cc/7XE2-XR3H].

219 *Id.* at 6.

220 *See* Haines et al., *supra* note 69 at 2.

221 *See Public Hacker Test on Swiss Post's E-Voting System*, SWISS POST (July 2, 2019), https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system [https://perma.cc/VL6B-TLEK].

222 "e-voting" is a more generic term than "Internet voting," and could refer to any kind of electronic voting system. I use it in this section only because Switzerland refers to its system this way. Since the Swiss Post "e-voting" system does do electronic return of the voted ballot through the internet from the voter's computer to the server computers, it is in fact an "Internet voting" system as I have defined the term.

223 Andrew Appel, *How the Swiss Post E-Voting System Addresses Client-Side Vulnerabilities*, FREEDOM TO TINKER (June 29, 2022), https://freedom-to-tinker.com/2022/06/29/how-the-swiss-post-e-voting-system-addresses-client-side-vulnerabilities/ [https://perma.cc/9YDY-DKHK].

224 *See* Haines *et al.*, *supra* note 69 at 1.

225 James Walker, *Swiss Post Puts E-Voting on Hold After Researchers Uncover Critical Security Errors*, THE DAILY SWIG (Nov. 26, 2019), https://portswigger.net/daily-swig/swiss-post-puts-e-voting-on-hold-after-researchers-uncover-critical-security-errors [https://perma.cc/G967-

redesign the trial phase of internet voting.[226] The Chancellery than commissioned independent scientists to do several separate studies and published their reports:[227]

- A *cryptographic protocol* study of the theoretical design, by experts in cryptography;
- A *systems security* study of the software itself, by an expert in operating systems security;
- *Infrastructure and operation* of the Swiss Post in running the system; and
- *Network security* of the internet voting infrastructure.

These reports are thorough and authoritative. Some of the scientists in question are world-renowned in their specific fields of expertise.[228] They were able to ask for clarifications and explanations from the software architects at Swiss Post.[229] The Chancellery estimates that these "independent experts … commissioned to conduct the examinations" will cost up to a million Swiss francs, by the time these and the next round of studies are complete.[230] That may seem like a lot, but in reading these reports it's clear that a lot of time and effort went into them—cryptographic protocols and software systems are complicated, and analyzing them takes a lot of time.

Swiss Post made the system architecture documentation and the source code available in a public repository.[231] That kind of transparency is admirable.

Before turning to the substance of the reports, I want to focus on the regulatory and legislative process. Internet-based election technology is complicated. Its security cannot be taken for granted; especially when scientific study after scientific study, decade after decade, demonstrates its insecurity. Of course, it might be

---

9PJ8].

[226] *E-Voting: Results of the First Independent Examination Available*, SWISS FEDERAL CHANCELLERY (Apr. 20, 2022), https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-88085.html [https://perma.cc/8BYW-KFZY] ("On 5 July 2021, the Federal Chancellery commissioned an independent examination of Swiss Post's e-voting system ….").

[227] *Id.*

[228] In my opinion.

[229] *See generally* SWISS FEDERAL CHANCELLERY, *supra* note 230.

[230] *See Redesign and Relaunch of Trials: Final Report of the Steering Committee Vote Électronique*, SWISS FEDERAL CHANCERY 1, 41-42 (Nov. 30, 2020), https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Final%20report%20SC%20VE_November%202020.pdf.download.pdf/Final%20report%20SC%20VE_November%202020.pdf [https://perma.cc/65C7-32TF].

[231] *See* SWISS POST E-VOTING, https://gitlab.com/swisspost-evoting [https://perma.cc/P2YM-YMVE].

possible that some new internet-voting system offered by some new vendor incorporates a previously unknown technology that is actually secure, but that would be an extraordinary claim that requires extraordinary evaluation. It is just that kind of intensive (and expensive) evaluation that the Swiss Chancellery commissioned in 2020. No American state has ever commissioned such an evaluation before adopting internet-voting products from vendors such as Voatz and Democracy Live. Instead, it is up to state election officials to accept the claims made by salesmen for election-system vendors; or in the case of the twenty states that do not permit any form of electronic ballot return, not to accept such claims.[232]

XIX. WHAT THE REPORTS SAID ABOUT THE SWISS POST SYSTEM

The critical vulnerabilities of an internet voting system are on the *client side* (i.e. hacked voter's computer) and the *server side* (i.e. hacked election computer).[233] On the server side, the Swiss Post system deploys *replication*—if the protocol works as intended, you'd have to hack *all* the replicated servers to corrupt the election; the mixnets (*see above*) ensure ballot privacy.[234] On the client side, the Swiss Post system defends against hacks using a different technology: a sheet of paper containing secrets known to the voter *but not to the voter's computer;* so that even if the voter's computer is hacked, it supposedly cannot make use of those secrets.[235]

For such a system to be secure, the underlying science must work, and the implementation of the system in actual software must be correct.

Before the reports even answer those questions, they point out: the engineers who build the system need to do a better job of documenting how the software, line by line, corresponds to the protocol it's supposed to be implementing.[236] That is,

---

[232] There is no process to cite. Since no state has commissioned such a study, we can assume that state election officials are not relying on such studies in making their decisions. The only such study commissioned by the Federal government is the SERVE report (Jefferson, cited above) which rejects security claims for an internet voting system. We can reasonably assume that, in the cases where election officials purchased a product or service, they relied in part on claims of serviceability by the vendors.

[233] I am speaking here as an expert in cybersecurity.

[234] *See* Thomas Haines et al., *supra* note 69 at 644 (pointing out that unfortunately the protocol did not work as intended).

[235] *See* Appel, *supra* note 223 (providing an explanation of how the secrets on the sheet of paper are supposed to provide cybersecurity). *See also* Andrew W. Appel, *Switzerland's E-Voting: The Threat Model*, FREEDOM TO TINKER (July 1, 2022), https://freedom-to-tinker.com/2022/07/01/switzerlands-e-voting-the-threat-model/ (explaining why this won't be as secure as its designers thought).

[236] Thomas Haines et al., *Report on the Swiss Post E-Voting System* 1, 1 (Mar. 24, 2022),

this kind of assessment can't work on an impenetrable black-box system; the Swiss Post developers have made good progress in "showing their work" so that it can be assessed, but they need to keep improving.[237]

Now, does the voting protocol work in principle? The experts on cryptographic voting protocols say,

> The Swiss Post e-voting system protocol documentation, code and security proofs show continuing improvement. The clarity of the protocol and documentation is much improved on earlier versions [which] has exposed many issues that were already present but not visible in the earlier versions of the system; this is progress. … There are, at present, significant gaps in the protocol specification, verification specification, and proofs. … [S]everal of the issues that we found require structural changes …. [238]

And, is the system architecture secure? The expert on system security says,

> the SwissPost E-voting system [has] been evolving … for well over a decade. … The current generation of the system under audit takes many important and valuable measures for security and transparency that are to this author's knowledge unprecedented or nearly-unprecedented among governmental E-voting programs worldwide. At a technical level, these measures include individual and universal verifiability mechanisms, trust-splitting of critical functions across four control components, the incorporation of an independent auditor role in the E-voting process, and the adoption of a reproducible build process for the E-voting software. [I see] ample evidence overall of both a system and a development process represent[ing] an exemplar that other governments worldwide should examine closely, learn from, and adopt similar state-of-the-art practices where appropriate.[239]

---

https://www.newsd.admin.ch/newsd/message/attachments/71147.pdf [https://perma.cc/9ZYL-L8EM] ("The Swiss Post e-voting system protocol documentation, code and security proofs show continuing improvement. The clarity of the protocol and documentation is much improved on earlier versions. This improved clarity has exposed many issues that were already present but not visible in the earlier versions of the system; this is progress. The project and system are highly complex and, for the moment, the review process is adding to the list of open questions rather than reducing it. There are, at present, significant gaps in the protocol specification, verification specification, and proofs. We continue to find issues which we had not noticed in previous iterations. And, as several parts of the system documentation remain missing, our evaluation could not consider the system in full. Furthermore, and as acknowledged by Swiss Post, several of the issues that we found require structural changes and additions to the current protocol. These protocol evolution steps require subtle cryptographic engineering and have an impact on the alignment between the protocol and the Ordinance on Electronic Voting (OEV), on the security proofs and on the code. These will in turn require new rounds of review.").

[237] *See id.*

[238] *Id.*

[239] Bryan Ford, *Auditing the Swiss Post E-voting System: An Architectural Perspective* 1, 2 (Apr. 4, 2022), https://www.newsd.admin.ch/newsd/message/attachments/71148.pdf [https://perma.cc/3AL7-QPZV].

But on the other hand, he says,

> the current system under audit is still far from the ideal system that … perhaps any expert well-versed in this technology domain – would in principle like to see. Some issues [include] the current system's reliance on a trusted and fully-centralized printing authority, and its exclusion of coercion or vote-buying as a risk to be taken seriously and potentially mitigated. [And] Explicit documentation of the architecture's security principles and assumptions, and how the concrete system embodies them, is still incomplete or unclear in many respects … The architecture's trust-splitting across four control components strengthens vote privacy, but does not currently strengthen either end-to-end election integrity or availability … The architecture critically relies on an independent auditor for universal verifiability, but the measures taken to ensure the auditor's independence appear incomplete … While the system's abstract cryptographic protocol is well-specified and rigorously formalized, the security of the lower-level message-based interactions between the critical devices – especially the interactions involving offline devices – do not yet appear to be fully specified or analyzed.[240]

In conclusion, the cryptographic-protocol experts recommend, "[w]e encourage the stakeholders in Swiss e-voting to allow adequate time for the system to thoroughly reviewed before restarting the use of e-voting,"[241] while the system-security expert concludes, "as imperfect as the current system might be when judged against a nonexistent ideal, the current system generally appears to achieve its stated goals, under the corresponding assumptions and the specific threat model around which it was designed."[242]

And what the Swiss authorities did after reading those reports was to indefinitely suspend the deployment of internet voting.[243]

Those thorough expert studies 2021–2022 missed a significant insecurity in the Swiss Post system that arose from new technological developments in 2022.[244] That's not their fault, of course, but it illustrates the extreme difficulty of continually securing an internet voting system.

XX. INTERNET VOTING LEGISLATION IN CALIFORNIA AND RHODE ISLAND

In 2022 both California and Rhode Island considered legislation that would direct their Secretaries of State to find a secure internet voting system and then deploy it.[245] In both states, election-security experts explained to legislators and

---

240 *Id.* at 2—3.

241 Haines et al., *supra* note 236, at 1.

242 Ford, *supra* note 239 at 21.

243 SWISS FEDERAL CHANCELLERY, *supra* note 226.

244 Appel, *Switzerland's E-Voting: The Threat Model*, *supra* note 235.

245 *See generally* S.B. 1480, 2022 Leg., Reg. Sess. (Ca. 2022) (introduced Feb. 18 2022, withdrawn

other policymakers that there is no such system, not with any currently known technology; there are only insecure systems.[246] In California, the sponsor withdrew the bill before a committee hearing.[247]

In Rhode Island, the bill passed and was signed into law.[248] The new Rhode Island statute attempts to achieve security by (for example) requiring compliance with the NIST Cybersecurity Framework.[249] But that Framework itself says,

> There sometimes is discussion about "compliance" with the Framework, and the Framework has utility as a structure and language for organizing and expressing compliance with an organization's own cybersecurity requirements. Nevertheless, the variety of ways in which the Framework can be used by an organization means that phrases like "compliance with the Framework" can be confusing and mean something very different to various stakeholders.[250]

Rhode Island also requires that whatever system is adopted "has had one or more independent security reviews.[251]" But *having* a review is one thing; the question is whether, as in Switzerland, (1) the review is truly independent; and (2) the results, if negative, will cause the regulatory authority (e.g., the Swiss

---

at the request of the author); 17 R.I. GEN LAWS ANN. § 17-20-6.1 (2021).

246 According to election-integrity advocates who have written privately to me.

247 S.B. 1480. "This bill would require a county elections official to permit a voter with a qualifying disability, as defined, to use a certified remote accessible vote by mail system that enables the voter to return a completed ballot electronically. The bill would permit the Secretary of State to certify this type of remote accessible vote by mail system and to develop procedures for a voter using the system to submit a signature electronically. Existing law imposes various restrictions on voting systems, generally, including that no part of the voting system shall be connected to the internet at any time. Existing law specifically prohibits a remote accessible vote by mail system from having the capability to use a remote server to mark a voter's selection transmitted to the server from the voter's computer via the internet, to store any voter identifiable selections on any remote server, or to tabulate votes. This bill would exempt the aforementioned remote accessible vote by mail system from these prohibitions only if, and to the extent that, these features are necessary for the operation of the system."

248 17 R.I. GEN LAWS ANN. § 17-20-6.1. "The secretary of state shall approve electronically transmitted ballots to and from eligible voters only through a service or solution that meets the following requirements: (1) The system has had one or more independent security reviews; (2) Demonstrates the system meets the National Institute of Standards and Technology (NIST) Cybersecurity Framework guidelines or federal cybersecurity framework guidelines of a successor designated federal agency or organization; and (3) Approved by the secretary of state."

249 *Id.*

250 *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. i, ii (Apr. 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018 [https://perma.cc/GTT3-EJXS].

251 17 R.I. GEN LAWS ANN. § 17-20-6.1.

Chancellery or the Rhode Island Secretary of State) to decertify the system.

XXI. BLOCKCHAIN

There's no insecurity of internet voting that blockchain does not make worse.[252]

XXII. HOW TO SERVE VOTERS WITH DISABILITIES

Citizens with disabilities have as much right to vote as anyone else, and our election systems should accommodate them. But is electronic ballot return, with its inherent insecurities, the way to do it? It is worth asking the voters themselves, how they vote and how they want to vote. And it turns out, most voters with disabilities voted by mail-in paper ballot in 2020 and want to continue voting that way.[253]

In the United States, out of 251 million resident adults, approximately[254]:

- 1.6% are in wheelchairs;

---

[252] NAT'L ACADS. OF SCI., ENG'G, & MED., *supra* note 36 at 103—05; *see also* Shawn M. Emery et al., *Penetration Testing a US Election Blockchain Prototype*, SIXTH INT'L JOINT CONF. ON ELEC. VOTING 82, 82—97 (2021), https://www.washingtonpost.com/context/penetration-testing-a-us-election-blockchain-prototype/1ca9f340-badd-4aa1-853d-1ffd4f8ef618/ [https://perma.cc/X6YL-5TZB]. (By 2020, the U.S. Postal Service had developed a prototype internet voting system based on Etherium blockchain, and (upon the advice of the Colorado National Cyper Security Center), asked Emery *et al.* (researchers at the University of Colorado, Colorado Springs) to conduct a security review. Emery *et al.* found many basic security flaws in the prototype, and concluded, "our research and related penetration testing of a blockchain based electronic voting system prototype has shown that a blockchain's strengths can also be its own weakness. …Technology alone currently does not meet the high assurances required for free and fair elections. Our hope is that this work will add to the body of knowledge of what and how an e-voting system that utilizes blockchain technology could and will be attacked.); Joseph Marks & Jacob Bogage, *USPS Built and Secretly Tested a Mobile Voting System Before 2020*, WASH. POST (Dec. 13, 2021), https://www.washingtonpost.com/nation/2021/12/13/usps-built-secretly-tested-mobile-voting-system-before-2020/ [https://perma.cc/2SS4-V6YH].

Emery *et al.*, do not identify which "U.S. government organization" commissioned them to study the prototype blockchain voting system, but the Washington Post identifies it as the Postal Service.

[253] *See generally* Lisa Schur & Douglas Kruse, *Disability and Voting Accessibility in the 2020 Elections: Final Report on Survey Results Submitted to the Election Assistance Committee*, Election Assistance Comm'n 1 (Feb. 16, 2021), https://www.eac.gov/sites/default/files/voters/Disability_and_voting_accessibility_in_the_2020_elections_final_report_on_survey_results.pdf [https://perma.cc/R386-2BX7].

[254] *See generally U.S. Census Report*, (2017), https://www2.census.gov/programs-surveys/popest/datasets/2010-2019/national/asrh/nc-est2019-alldata-r-file16.csv [https://perma.cc/EXM6-3GCX] (showing in July 2017, the U.S. resident 18+ population was 251,400,193).

- 2.9% million have difficulty grasping objects[255]; and
- 0.4% are legally blind[256].

A report commissioned by the Election Assistance Commission[257] provides very useful information. Voting difficulties for people with disabilities declined markedly from 2012 to 2020, mostly because of the large pandemic-related shift to mail-in ballots.[258] In 2020, 83% of voters with disabilities voted independently without any difficulty, and 89% were able to vote (independently or with assistance) without difficulty; this compares to 94% of voters without disabilities who were able to vote without difficulty.[259]

The percentage of voters who said that voting at a polling place was "very easy" was almost identical in 2020 between voters with and without disabilities (82% versus 83%).[260] The percentage who said voting on mail-in ballots was "very easy" was also almost identical (79% versus 81%).[261] However, only 64% of those with vision impairments said it was "very easy" to vote by mail.[262]

Regarding the ability to vote independently, only 6% of voters with disabilities needed assistance at a polling place, and 5% needed assistance completing their mail-in ballot; but 11% needed assistance in returning the ballot.[263] 16% of voters with vision impairment needed assistance in the polling place.[264] Of all voters with disabilities who needed assistance in the polling place, only 83% actually received assistance.[265]

Almost all of these numbers were significantly better in 2020 than in 2012. Either the U.S. has made progress in accommodating voters with disabilities, or the general shift to mail-in ballots accommodates the needs of those voters, or both. In

---

255 Kristina A. Theis et al., *Which One? What Kind? How Many? Types, Causes, and Prevalence of Disability Among U.S. Adults*, 12 Disability & Health J. 411, 414 (2019).

256 *See* Abraham D. Flaxman et al., *Prevalence of Visual Acuity Loss or Blindness in the US, A Bayesian Meta-Analysis*, 139 JAMA Ophthalmology 717, 721 (2021) (showing in 2017, the U.S. legally blind 18+ population was 1,052,332, (that is, best-corrected visual acuity in the better-seeing eye worse than 20/200 vision)).

257 *See* Schur & Kruse *supra* note 253 at 1.

258 *Id.*

259 *Id.* at 10.

260 *Id.* at 32.

261 *Id.*at 8.

262 *Id.*

263 *Id.* at 5.

264 *Id.* at 9.

265 *Id.*

2020, people with disabilities voted at a 7% lower rate than people of the same age without disabilities.[266]

About 8% of voters with disabilities want to vote fully online by smartphone or computer, compared to 12% of voters without disabilities.[267] Among voters with vision impairment, only 2% wanted to vote this way.[268] Among nonvoters, 27% of those with disabilities (9% of those with vision impairment) and 20% of those without disabilities want to vote online. [269]

That is, voters with disabilities desire internet voting even less than voters without disabilities. Internet voting is not the way to serve these voters.

XXIII. CONCLUSION

Internet voting is attractive, and it is clear why: some people have difficulty coming to the polls (if they live overseas or have disabilities), the mail is slow (for conventional absentee balloting), and the internet is convenient. There is often public pressure to adopt internet voting. But internet voting is subject to a unique danger to which other methods are not vulnerable: that a single criminal actor without even a local physical presence could hack enough computers to change thousands of votes and alter the results of local or national elections.

One might ask, but suppose we limit internet voting to a smallish class of voters, such as those abroad or those with disabilities? Are we saying that it's all right if only *their* thousands of votes are stolen? And there is a slippery slope: once internet voting is normalized for one class of voters, other classes will demand it. We have already seen evidence of this: first UOCAVA voters, then voters with disabilities.

In this new era where many voters are suspicious of the integrity of elections, we must run elections with as much transparency and integrity as we can. In the current state of scientific knowledge in the field of election security, that means paper ballots directly marked by the voter and recountable by hand. In the realm of public trust, that also means paper ballots directly marked by the voter and recountable by hand.

---

266 *Id.* at 1.

267 *Id.*

268 *Id.* at 12.

269 *Id.*