INNOVATIONS IN INTERNET VOTING SYSTEMS

Michelle Mount*

CITE AS: 4 GEO. L. TECH. REV. 699 (2020)

TABLE OF CONTENTS

I. INTRODUCTION

Election technology is democracy's critical infrastructure and must withstand manipulation from inside and outside forces. But in recent years, contested recounts have raised procedural questions. Reports issued on Russia's attempts to influence the 2016 presidential election reveal other system vulnerabilities.[1] Security experts and the House of Representatives have called for a return to paper ballots.[2] But some states are exploring how

* Georgetown University Law Center, J.D. Candidate 2020; Boston University, B.S. Business and Finance. My sincerest gratitude goes out to the fabulous *GLTR* editors, without whom this piece would not have been possible.

[1] S. SELECT COMM. ON INTELLIGENCE, 116TH CONG., RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE WITH ADDITIONAL VIEW, S. REP. NO. 116-XX (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [https://perma.cc/L2KW-E42L].

[2] SAFE Act, H.R. 2722, 116th Cong. (2019–2020), https://www.congress.gov/bill/116th-

Internet voting and advances in blockchain technology, facial recognition software, and cryptography could improve the election process.

This explainer (1) describes Internet voting and its inherent challenges, (2) analyzes the United States' traditional Internet voting system, and (3) examines the benefits and risks of novel systems being implemented in the United States and around the world.

II. THE INVENTION OF INTERNET VOTING AND ITS INHERENT CHALLENGES

The late 1990s brought the cheap personal computing technology and widespread Internet access that fueled countries' first experiments with Internet voting.[3] Internet voting systems allow voters to cast their votes online, using a computer or mobile device, in a remote and unsupervised location.[4] But this label applies to a broad range of solutions, and none have gained universal acceptance. The systems vary widely because the feasibility of each system depends on each jurisdiction's Internet access, priorities, budget, laws, and election risk, as well as the digital literacy of its voters. Additionally, the election process has discrete phases: ballot distribution, voter identity verification, ballot casting, vote tallying, and vote auditing.[5] Governments may choose to perform all or some of these phases over the Internet.[6]

The technological challenges are formidable; some would say insurmountable.[7] Election tampering is increasingly prevalent,[8] and a

---

congress/house-bill/2722/text [https://perma.cc/BQ84-FDSU]; Lawrence Norden & Andrea Córdova McCadney, *Voting Machines at Risk: Where We Stand Today*, BRENNAN CTR. JUST. (Mar. 5, 2019), https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today [https://perma.cc/S3R8-8DTG].

[3] U.S. ELECTION ASSISTANCE COMM'N, A SURVEY OF INTERNET VOTING 6 (Sept. 14, 2011), https://www.verifiedvoting.org/wp-content/uploads/2014/09/EAC_2011_SIV_FINAL.pdf [https://perma.cc/Y4UV-45FW].

[4] *See* NAT'L DEMOCRATIC INST., COMMON ELECTRONIC VOTING AND COUNTING TECHNOLOGIES (last updated Dec. 17, 2013), https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies [https://perma.cc/SPM5-MGD7] (defining Internet voting, generally).

[5] JOSEPH R. KINIRY ET AL., THE FUTURE OF VOTING 18 (July 2015), https://people.csail.mit.edu/rivest/pubs/OVF15.pdf [https://perma.cc/5522-NZMM] (describing the phases and steps in an election process).

[6] U.S. ELECTION ASSISTANCE COMM'N, *supra* note 4, at 8–10 (illustrating various "Internet voting channels" and discussing the steps that various systems perform online).

[7] David Jefferson, *If I Can Shop and Bank Online, Why Can't I Vote Online?* VERIFIED VOTING (last visited Nov. 5, 2019), https://www.verifiedvoting.org/resources/internet-voting/vote-online/#fn-47671-1 [https://perma.cc/WN7H-J8AF] ("There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future.").

[8] COMMUNICATIONS SECURITY ESTABLISHMENT OF CANADA, CYBER THREATS TO CANADA'S

networked voting system must withstand hacks of unprecedented sophistication and power.[9] Some voters worry more about interference by their own government. Thus, an optimal voting system offers transparency so that a voter can verify that their vote was counted if they distrust the system's operator.[10] At the same time, the system must guarantee voter privacy to prevent bribery and voter intimidation.[11] The cost of a manipulated election is enormous, and the coded nature of computer language makes subversion difficult to detect.[12] Furthermore, advanced encryption techniques must be used to ensure that voters are not vulnerable to hacks and identity fraud.[13]

III. THE HISTORICAL INTERNET VOTING SYSTEM USED IN THE UNITED STATES

Currently, Internet voting is only available for some overseas military service members and other select citizens[14]: since 1986 states have been required to provide absentee ballots to overseas members of the military,[15] but they are not required to accept those ballots electronically.[16] The group is relatively small: in 2016 over 100,000 votes were cast online.[17] There is still not a federally implemented secure voting solution for overseas military personnel and a twelve-year initiative to research such a system was repealed in 2015.[18] The result is a piecemeal solution. Nineteen states and the District of Columbia accept some absentee ballots via email, and four states allow some voters to return ballots using a web-based portal.[19]

While these technologies are comparatively inexpensive and easy to

---

DEMOCRATIC PROCESS 16 (2019), https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf [https://perma.cc/SH8K-2HPG].

[9] Jefferson, *supra* note 7.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Electronic Transmission of Ballots*, NAT'L CONF. ST. LEGISLATURES (Sept. 5, 2019), http://www.ncsl.org/research/elections-and-campaigns/Internet-voting.aspx [https://perma.cc/5SGP-G28H].

[15] *The MOVE Act*, U.S. DEP'T OF JUSTICE (Oct. 21, 2010), https://www.justice.gov/archives/opa/blog/move-act [https://perma.cc/6K6T-DWVG].

[16] *Internet Voting*, VERIFIED VOTING (2018), https://www.verifiedvoting.org/resources/Internet-voting/#fn-45112-1 [https://perma.cc/T6QJ-V9DK] (discussing the reasons the MOVE Act is "notably silent on the subject of return of voted ballots").

[17] SUSAN GREENHALGH ET AL., EMAIL AND INTERNET VOTING 5 (2018), https://www.commoncause.org/wp-content/uploads/2018/10/ElectionSecurityReport.pdf [https://perma.cc/AA36-338N].

[18] Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 593, 128 Stat. 3,292, 3,395 (2014).

[19] *Electronic Transmission of Ballots*, *supra* note 14.

administer, the risks are numerous.[20] First, they compromise voter privacy—most states require online voters to waive their right to a secret ballot.[21] Ballots submitted from another country move through networks of routers and forwarding agents before arriving at American election officials.[22] Transmitted data can be viewed by national intelligence agencies.[23] Second, ballots can be manipulated while in transit and detecting forged ballots is nearly impossible.[24] Third, voters' personal devices may be infected with malware, and the ballot files could carry malware into the election network.[25] Security analysts caution that because these are risks inherent in the system architecture, they are unlikely to be remedied by encryption, firewalls, strong passwords, or voter signature checking.[26]

IV. CURRENT CONFIGURATIONS OF NEW INTERNET VOTING SYSTEMS

The United States is not alone in its election security concerns. A report by the Canadian government found: "In 2018, half of all advanced democracies holding national elections had their democratic process targeted by cyber threat activity. This represents about a threefold increase since 2015."[27] These growing concerns about election legitimacy have sparked innovative solutions to address voter registration, system transparency, and ballot privacy.

This section provides a general introduction to four different types of Internet voting systems being used around the world. Part A discusses the world's oldest nation-wide Internet voting system, which is infrastructure intensive and depends heavily on the legitimacy of the Estonian government for its legitimacy. In contrast, Part B reviews Scytl's internet voting software, which offers end-to-end verifiability. Part C explores a blockchain-backed Internet voting system that was piloted in Russia. Finally, Part D looks at the

---

[20] Jordi Puiggali, *Remote Voting Schemes: A Comparative Analysis,* SCYTL 19 (Oct. 2007), https://www.scytl.com/wp-content/uploads/2013/04/Remote_Voting_Schemes_A_comparative_analysis.pdf, [https://perma.cc/D8WF-YHA5] (illustrating a comparative analysis of system performance in election management).

[21] CAITRIONA FITZGERALD ET AL., THE SECRET BALLOT AT RISK: RECOMMENDATIONS FOR PROTECTING DEMOCRACY 8 (2016), https://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf [https://perma.cc/4LW6-7DY8].

[22] GREENHALGH ET AL., *supra* note 17, at 10.

[23] *What About Email and Fax?*, VERIFIED VOTING (last visited Nov. 5, 2019), https://www.verifiedvoting.org/resources/internet-voting/email-fax/ [https://perma.cc/BR4W-QRBL].

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Communications Security Establishment of Canada*, *supra* note 8.

smartphone-accessible system with biometric registration which is being piloted in the U.S. Together, these examples highlight the key tradeoffs and considerations at play in the design and implementation of Internet voting systems.

A. Estonia's Fully Digitalized E-Government System

Estonia has one of the most digitalized governments in the world,[28] and in 2005, it became the first country to use Internet voting nationally.[29] Its voting system draws on the country's robust digital infrastructure. Most of the country's public services are available online and accessible with citizen's digital ID cards.[30] One of core strengths of Estonia's voting system is the pervasiveness of its national ID infrastructure and the sophistication of its cryptographic facilities.[31]

Estonia's unique system uses digital identification to provide authenticated access to its comprehensive e-government system, which allows citizens online access to almost all public services.[32] The different information systems are connected through a secure Internet-based data exchange layer called the X-Road.[33] The data is stored on servers run by the Estonian government that are located in both Estonia and Luxembourg.[34] But the system's critical registries are backed up on the private KSI blockchain.[35] Because the KSI blockchain only stores coded references to the data, the raw

---

[28] In 2007, Estonia was the victim of a devastating three-week cyberattack launched out of Russia, deemed Cyber War I. Afterwards, Estonia began to develop an expertise in defensive strategies. Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, 9 EUR. AFF. (Winter/Spring 2008), https://www.europeaninstitute.org/index.php/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia?tmpl=component&print=1 [https://perma.cc/45WK-HE4H]; *see* KRISTJAN VASSIL, ESTONIAN E-GOVERNMENT ECOSYSTEM 2 (June 2015), http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf [https://perma.cc/43L3-ADPV] (describing the country as being at the forefront of states in modernizing governance).

[29] DREW SPRINGALL ET AL., SECURITY ANALYSIS OF THE ESTONIAN INTERNET VOTING SYSTEM 1 (Nov., 2014), https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [https://perma.cc/T4MU-EL2N].

[30] VASSIL, *supra* note 28, at 2.

[31] *See* VASSIL, *supra* note 28, at 3–7; SPRINGALL ET AL., *supra* note 29, at 2, 10.

[32] *See* E-ESTONIA (last visited Nov. 5, 2019), https://e-estonia.com [https://perma.cc/D24J-VB5G].

[33] VASSIL, *supra* note 28, at 11.

[34] *Data Embassy,* E-ESTONIA (last visited Nov. 5, 2019), https://e-estonia.com/solutions/e-governance/data-embassy [https://perma.cc/N8VZ-QNDT].

[35] *Id.*

data does not need to transfer out of Estonia's system.[36] This private blockchain also provides a method of independent verification, which safeguards against government manipulation.[37]

Each Estonian with voting rights is issued an electronic national ID, or Mobile-ID, which facilitates authentication, encryption, and digital signatures when used within the voting software.[38] Voters insert their digital ID into a card reader that connects with their computer and downloads the voting software.[39] Once a vote is cast, a collector program verifies the vote and sends it to a processer program to be anonymized for counting.[40] An organizer program then decrypts the votes using a private key and tallies them.[41] The votes are then audited and voters can verify that their vote was recorded appropriately.[42]

Estonia's system is popular; in their 2019 European Parliament election, 46.7% of voters cast their ballots online.[43] But critics assert that the system is not sufficiently transparent[44] and that there are security issues.[45] Because the programs performing the key monitoring and authentication roles are managed on government servers,[46] citizens must have considerable trust in the government running and protecting the elections.[47] Additionally, the startup and maintenance costs of Estonia's digital ID infrastructure would be costly.[48] But proponents of digitalization argue that investing in a system

---

[36] *Keyless Signature Infrastructure*, GUARDTIME FEDERAL (last visited Nov. 5, 2019), http://www.guardtime-federal.com/ksi/ [https://perma.cc/NL6E-9JXL].
[37] *Id.*
[38] STATE ELECTORAL OFFICE OF ESTONIA, GENERAL FRAMEWORK OF ELECTRONIC VOTING AND IMPLEMENTATION THEREOF AT NATIONAL ELECTIONS IN ESTONIA 4–6 (June 20, 2017), https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf [https://perma.cc/HS5U-YXKC].
[39] *Requirements to the Voter and Their Computer*, VALIMISED (last visited Nov. 5, 2019), https://www.valimised.ee/en/Internet-voting/requirements-voter-and-their-computer [https://perma.cc/QM27-B2N8].
[40] STATE ELECTORAL OFFICE OF ESTONIA, *supra* note 38, at 9.
[41] *Id.*
[42] *Id.*
[43] *Statistics About Internet Voting in Estonia*, VALIMISED (last visited Nov. 5, 2019), https://www.valimised.ee/en/archive/statistics-about-Internet-voting-estonia [https://perma.cc/8LDY-PRE7].
[44] SPRINGALL ET AL., *supra* note 29, at 2.
[45] *See* Barbara Simons, *Why Internet Voting Is Dangerous*, 4 GEO. L. TECH. REV. 543 (2020); Barbara Simons, *Verified Voting Blog: Report on the Estonian Internet Voting System*, VERIFIED VOTING (Sept. 3, 2011), https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/ [https://perma.cc/Q5UM-3MGV].
[46] STATE ELECTORAL OFFICE OF ESTONIA, *supra* note 38, at 9.
[47] SPRINGALL ET AL., *supra* note 29, at 2.
[48] KINIRY ET AL., *supra*, note 5, at 113 ("Voters could be issued cryptographic ID cards such

which provides an authenticated digital identity may reduce others costs, such as the economic cost of fraud or of personnel to oversee laborious recounts.[49]

B. Scytl's End-to-End Verifiable Voting System[50]

Scytl is a Barcelona-based software company that has facilitated online voting in more than 42 countries.[51] Most notably, Switzerland, a pioneer in the Internet voting space since 2000, retained Scytl in partnership with its online election facilitator and postal service company, Swiss Post.[52] Scytl offers an end-to-end verifiable voting solution,[53] which solves the intrinsic problem of providing "public evidence from secret ballots."[54] End-to-end verifiability

---

as the CAC cards issued to DoD personnel or like the national ID card of Estonia. … [But] the startup and maintenance costs will be very high. Voters would have to buy computers or devices that could read the cards, and they would almost certainly have to be useful for other online purposes besides just voting in order to justify the costs involved to both the government and the voter."); *see also Internet Voting in Estonia (iVote)*, JOINUP (Apr. 24, 2007), https://joinup.ec.europa.eu/collection/eparticipation-and-evoting/document/Internet-voting-estonia-ivote [https://perma.cc/RQC8-ZYQD] ("[Had there] not been a national population register or an authentication system using ID cards, the Internet elections in Estonia would have been very costly.").

[49] *Internet Voting in Estonia, supra* note 47 (noting that paper ballots are the most expensive voting method for those abroad and that replacing them with electronic votes will reduce costs); *see also* Jane Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 799 (2017) (describing how trustless systems in theory reduce transaction costs).

[50] As this issue was going to publication, Scytl entered bankruptcy proceedings. The outcome of those proceedings is unclear, but the underlying technology remains relevant. This Technology Explainer will therefore refer to Scytl as an ongoing project. For news stories about Scytl's bankruptcy, see Sonia Fenazzi, *Swiss Post Set to Re-Launch Its E-Voting System*, SWISS INFO (June 9, 2020, 10:45 AM), https://www.swissinfo.ch/eng/swiss-post-set-to-relaunch-its-e-voting-system/45820842 [https://perma.cc/P7PY-9UWR]; *El Juze Abre La Venta De Scytl y Espera Ofertas Por La Empresa Hasta El 22 De Junio*, LA VANGUARDIA (June 8, 2020, 10:42 AM), https://www.lavanguardia.com/economia/20200607/481657532094/scytl-subasta-unidad-productiva-venta-indra-liquidacion.html [https://perma.cc/2NEA-HPT4].

[51] Press Release, Scytl, OAS Staff Federal Credit Union Leverage Online Voting to Elect the Board of Directors and Credit Committee (Aug. 24, 2016), https://www.scytl.com/wp-content/uploads/2016/08/press-release-oas-online-voting-august-2016.pdf [https://perma.cc/5STA-LW6F].

[52] *Partners: Swiss Post*, SCYTL, https://www.scytl.com/en/partners/swiss-post/ [https://perma.cc/W4TU-GJEU].

[53] MASSIMILIANO CLAPS & PHILIP CARTER, TECHNOLOGY SPOTLIGHT: DELIVERING END-TO-END ELECTION MODERNIZATION ROADMAPS 12 (Sept. 2013), https://www.scytl.com/en/resource/white-paper-idc-technology-spotlight-delivering-end-end-election-modernization-roadmaps/ [https://perma.cc/TY3L-UWAS].

[54] *See generally* Matthew Bernhard et al., *Public Evidence from Secret Ballots, in* 10615

allows the voter to (1) check that their vote was recorded correctly, (2) check that their vote was included in the final tally, and (3) double-check that their vote was counted in the votes announced in the election outcome.[55] This means that voters can have confidence in the system without having to trust the election officials. This verification system is complex; it requires the system to use advanced encryption techniques while still allowing voters to access their data at each stage.[56]

Scytl's system accomplishes end-to-end verifiability through a sequence of cryptographic measures. Once the vote is cast the ballot is immediately encrypted on voter's device, instead of in transmission.[57] Next, the ballot is sent to Scytl and privacy is ensured through use of cryptographic mixnets.[58] Mixnets—mix networks—are generally used to make communication between sending and receiving networks untraceable.[59] To do this, they shuffle messages and forward them to the next destination (possibly another node in the mix network) in a random order.[60] Mixnets anonymize the voter's identity by shuffling the data and breaking the original voting order in a process that re-encrypts and then decrypts the votes.[61] Finally, voters can use the return codes they receive on their devices to check the public Bulletin Board and verify that their vote was properly recorded.[62] Also during this stage, independent auditors or the media can observe and verify the vote counting and vote decryption process.[63]

Scytl's system, though, has notable drawbacks. One issue is that Scytl's system does not address the problem of secure voter registration.[64] Scytl requires governments to have already registered voters securely and to

---

LECTURE NOTES IN COMPUTER SCIENCE 84–109 (R. Krimmer et al. eds., 2017), https://arxiv.org/pdf/1707.08619.pdf [https://perma.cc/NHL2-F395] (coining the phrase to describe the problem that end-to-end verifiability solves).

[55] KINIRY ET AL., *supra* note 5, at ii.

[56] FAYAZ KHAKI, IMPLEMENTING END-TO-END VERIFIABLE ONLINE VOTING FOR SECURE, TRANSPARENT AND TAMPER-PROOF ELECTIONS 6 (Oct. 2014), https://www.scytl.com/en/resource/white-paper-idc-implementing-end-end-verifiable-online-voting-secure-transparent-tamper-proof-elections/ [https://perma.cc/T4U9-AFTB].

[57] *See id.* at 3.

[58] *See id.*

[59] CLAUDIO A. ARDAGNA ET AL., *Privacy Preservation Over Untrusted Mobile Networks*, *in* PRIVACY IN LOCATION-BASED APPLICATIONS RESEARCH ISSUES AND EMERGING TRENDS 88 (Claudio Bettini et al. eds., 2009).

[60] *Id.*

[61] KHAKI, *supra* note 54.

[62] *Solution Overview Online Voting End-to-End Security and Verifiability*, SCYTL (last visited Nov. 5, 2019), https://www.scytl.com/en/resource/solution-overview-online-voting-end-end-security-verifiability/ [https://perma.cc/K8YQ-LBDV].

[63] KHAKI, *supra* note 54, at 4.

[64] *See* GREENHALGH ET AL., *supra* note 17, at 13.

have issued one-use digital certificates or electronic ID cards to access the system.[65] Additionally, some experts cite older studies of other end-to-end verifiable systems arguing that such systems are "complex and notoriously difficult to use," and worry that this could disincentivize voters.[66]

Finally, researchers found security flaws in Scytl's software. The first of these flaws was a "cryptographic trapdoor" that would have allowed a malignant entity to insert or remove votes while votes are shuffled in the mixnet.[67] Even though that first issue may have been corrected, this same group of researchers found an additional issue in the decryption process.[68] Security developments are ongoing.[69]

C. Russia's Recent Pilot of an Ethereum Blockchain-backed Voting System

In 2019 Russia hosted one of the largest ever tests of a blockchain-

---

[65] KHAKI, *supra* note 54, at 4.

[66] GREENHALGH ET AL., *supra* note 17, at 13 (citing Claudia Z. Acemyan et al., *Useability of Voter-Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Pret-a-Voter, and Scantegrity II*, 2 USENIX J. ELECTION TECH. & SYS. 3 (2014)).

[67] *See* Sarah Jamie Lewis, Olivier Pereira, & Vanessa Teague, *Ceci N'est Pas Une Preuve: The Use of Trapdoor Commitments in Bayer-Groth Proofs and The Implications for the Verifiabilty of The Scytl-Swiss Post Internet Voting System* (Mar. 12, 2019), https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf [https://perma.cc/4JQA-ER8A]; *see also* SARAH JAMIE LEWIS, OLIVIER PEREIRA, & VANESSA TEAGUE, TRAPDOOR COMMITMENTS IN THE SWISS POST E-VOTING SHUFFLE PROOF (2019), https://people.eng.unimelb.edu.au/vjteague/SwissVote [https://perma.cc/C497-LAJP] (website-style report hosted by the University of Melbourne) .

[68] *See* Vanessa Teague, *What a Second Flaw in Switzerland's sVote Means for NSW's Vote*, PURSUIT (Mar. 25, 2019), https://pursuit.unimelb.edu.au/articles/what-a-second-flaw-in-switzerland-s-svote-means-for-nsw-s-ivote [https://perma.cc/8SRV-7TD2]; Sarah Jamie Lewis, Olivier Pereira, & Vanessa Teague, *How Not to Prove Your Election: The Use of Non-Adaptive Zero Knowledge Proofs in The Scytl-Swiss Post Internet Voting System and Its Implications for Decryption Proof Soundness* (Mar. 25, 2019), https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf [https://perma.cc/Z9GT-7ZP5].

[69] Scytl's bankruptcy has complicated these developments. But Swiss Post, which previously used Scytl's technology and focused on that technology during a public intrusion test in 2019, appears intent on continuing to develop Internet voting systems. *See generally E-Voting: Online Voting and Elections*, POST.CH, https://www.post.ch/en/business-solutions/e-voting [https://perma.cc/XPM9-GHVN]; *see also* Press Release, Swiss Post Error in The Source Code Discovered and Rectified (Mar. 12, 2019), https://www.post.ch/en/about-us/media/press-releases/2019/error-in-the-source-code-discovered-and-rectified [https://perma.cc/SW6C-4GQD]; PIT MANAGEMENT COMMITTEE, SWISS POST, FINAL REPORT: PUBLIC INTRUSION TEST (2019), https://www.post.ch/en/business-solutions/e-voting/publications-and-source-code#public-intrusion-test-2019 [https://perma.cc/X8RA-7EMV].

based Internet voting system in a binding national election during its parliamentary elections in Moscow.[70] The system required voters to register online through their existing mos.ru account or apply in person with their passport.[71] The mos.ru account is a government web portal where citizens can access certain services. Upon accessing the ballot, the voter was prompted to enter a confirmation code that they subsequently received via SMS at the mobile number connected to their account.[72] The voter then had fifteen minutes to cast their vote. In theory, voters could verify their vote online.[73] But a security assessment found that "the verifiability properties were not as strong as what could be hoped for from a blockchain-based ledger."[74]

The system used smart contracts on a specific permissioned Ethereum blockchain.[75] After voting, the encrypted ballots are not stored in the web portal;[76] they are immediately recorded on the blockchain as transactions, one transaction per ballot.[77] Users are given enough information to identify their ballot was recorded on the blockchain, and the other ballots remain encrypted.[78] This configuration was designed to allow a voter to access only their own vote to ensure it was properly recorded.[79]

More than 10,000 people used this Internet voting system.[80] Although the system did not use mixnets, security experts found that the encryption was significantly hard to break.[81] Even so, the system could not guarantee ballot secrecy.[82] This is because, during the election, the blockchain holding the encrypted voting data was still web-accessible for few hours.[83] And at the end of the election day, the private key was sent to the web-accessible blockchain for verifiability purposes.[84] Analysts were then able to obtain this private key

---

[70] *Electronic Elections*, MOSCOW MAYOR OFFICIAL WEBSITE (last visited Nov. 5, 2019), https://www.mos.ru/en/city/projects/blockchain-vybory/ [https://perma.cc/4GXZ-L6WC].
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] PIERRICK GAUDRY & ALEXANDER GOLOVNEV, BREAKING THE ENCRYPTION SCHEME OF THE MOSCOW INTERNET VOTING SYSTEM 8 (2019), https://golovnev.org/papers/election.pdf [https://perma.cc/5LPC-SFS7].
[75] *Id.* at 2, 8. The Ethereum blockchain records data when it is authenticated by consensus of the network nodes.
[76] *Electronic Elections*, *supra* note 65.
[77] GAUDRY & GOLOVNEV, *supra* note 69, at 7.
[78] *Id.* at 9.
[79] *Id.* at 7.
[80] *Id.* at 9.
[81] *Id.*
[82] *Id.* at 9–10.
[83] *Id.* at 9.
[84] *Id.*

and use it to decrypt 9,810 ballots.[85] This prompted government concerns about expanding the system,[86] and the losing candidate intends to challenge the election outcome in court.[87]

D. The United States' Pilot of a Smartphone-Voting System Using Biometric Registration

A new type of smartphone-accessible Internet voting system was piloted in West Virginia's 2018 primary elections.[88] This system can authenticate voters through biometrics and therefore does not require an alternative digital ID. After receiving their absentee ballot, voters are instructed to download Voatz's mobile app,[89] which requires them to scan in their state driver's license or passport, take a moving selfie, and touch the fingerprint reader.[90] Using facial recognition technology, Voatz verifies whether the selfie matches the government ID, and if it does, the ID holder is eligible to vote.[91] The app registers the mobile device to the voter's fingerprint.[92] This connection ensures that a voter can vote only on one device and that a device can be used by only one voter.[93] Once this linkage is established, it is encrypted and the identifying information is deleted. The system preserves ballot secrecy with end-to-end encryption and immutably records the votes on a multi-node Hyperledger-based permissioned blockchain. [94]

So far Voatz has withstood attempted hacks and limited pilots have been successful.[95] The West Virginia pilot included 147 military absentee

---

[85] *Id.* at 9–10.
[86] Elena Rozhkova et al., *Tsifroi Ne Sklad'ibaetsia* [The Numbers Don't Add Up], KOMMERS. (Sept. 17, 2019), https://www.kommersant.ru/doc/4095101 [https://perma.cc/XLH6-2BAE].
[87] Elena Rozhkova, *Nastroenie Sboevoe* [A Failing Mood], KOMMERS. (Sept. 9, 2019), https://www.kommersant.ru/doc/4088592 [https://perma.cc/4HNE-537D].
[88] *Frequently Asked Questions (FAQ)*, VOATZ, https://voatz.com/faq.html#wv-pilot [https://perma.cc/56LU-UQJD].
[89] *See id.* (explaining how voters can register and vote).
[90] LARRY MOORE & NIMIT SAWHNEY, UNDER THE HOOD: THE WEST VIRGINIA MOBILE VOTING PILOT 3 (2019) https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf [https://perma.cc/X6GM-3ZKU].
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] NAT'L. CYBERSECURITY CTR., THE DENVER MOBILE VOTING PILOT 6 (2019), https://cyber-center.org/wp-content/uploads/2019/08/Mobile-Voting-Audit-Report-on-the-Denver-County-Pilots-FINAL.pdf [https://perma.cc/9GLQ-XQQX].
[95] Statement from Mike Stuart, U.S. Attorney for the S. Dist. of W. Virginia, on Election Security (Oct. 2, 2019), https://www.justice.gov/usao-sdwv/pr/united-states-attorney-mike-stuart-issues-statement-election-security [https://perma.cc/X5M5-4L2Y].

voters.[96] In Denver, Colorado's 2019 pilot for its municipal elections, 232 ballots were returned and counted. [97] For the first time, Internet voting made available to local citizens with disabilities in Utah County, Utah's 2019 pilot.[98] And in October 2019, two counties in Oregon announced their intention to pilot the system for overseas military voters.[99]

V. CONCLUSION

There is no one-size-fits-all Internet voting solution. Some robust systems may be too costly. Skeptical voters may demand more verifiability. Transparent blockchain systems may not be able to guarantee privacy. And managing the voter registration process and data security continues to be challenging. Regardless, the potential gains in election legitimacy and security motivate governments to persist in testing solutions. And in the age of online-banking and shopping, voters are growing increasingly irritated by long voting lines and their questionably disparate socio-economic impact on voter turnout.[100] Under mounting pressure from governments and voters, the innovation in Internet voting is likely to continue.

---

[96] MOORE & SAWHNEY, *supra* note 85, at 6.

[97] NAT'L. CYBERSECURITY CTR., *supra* note 89, at 8.

[98] Benjamin Freed, *Utah County, Utah, Begins Review of Mobile-app Votes*, STATESCOOP (Sept. 4, 2019), https://statescoop.com/utah-county-utah-begins-review-of-mobile-app-votes/ [https://perma.cc/55AK-WKU5].

[99] Andrew Selsky, *2 Oregon Counties Offer Vote-by-Mobile to Overseas Voters*, ASSOCIATED PRESS Oct. 16, 2019, https://apnews.com/8ce0fbc400514f55839fa84fb364d7f4.

[100] Bill Hewitt, *Online Voting and Democracy in the Digital Age*, CONSUMER REP. (May 17, 2016), https://www.consumerreports.org/online-voting/online-voting-democracy-in-the-digital-age/ [https://perma.cc/24MA-JA4C] ("A 2016 survey of voting-age Americans revealed that 33 percent would be more likely to vote if they could do it from an Internet-connected device like a smartphone.").