

April 9, 2020

Dear Governors and State Election Directors,

In light of the unprecedented challenge to American elections presented by the COVID-19 pandemic, we are writing to share information on the scientific evidence regarding the security of internet voting. **Internet voting is not a secure solution for voting in the United States, nor will it be in the foreseeable future. We urge you to refrain from allowing the use of any internet or voting app system and consider expanding access to voting by mail and early voting** to maintain the security, accuracy, and voter protections essential for American elections in the face of this public health crisis.

As you know, there is little time to spare to assure full, fair and timely elections across the United States in November of 2020. We make this request -- with full knowledge of the profound challenges you face to assure all Americans' ability to vote in a time of pandemic -- for the reasons documented in the attached letter prepared by the American Association for the Advancement of Science Center for Scientific Evidence in Public Issues and endorsed by leading organizations and experts in cybersecurity and computing. In sum, those reasons are:

- **All internet voting systems and technologies are currently inherently insecure.**
- **No technical evidence exists that any internet voting technology is safe or can be made so in the foreseeable future; rather, all research performed to date demonstrates the opposite.**
- **No blockchain technology can mitigate the profound dangers inherent in internet voting.**
- **No mobile voting app is sufficiently secure to permit its use.**

As detailed in the attached letter, these statements reflect the findings of both recent and two decades of rigorous, science-based analysis by, among many others: the National Academies of Science, Engineering, and Medicine; officials at the Department of Homeland Security; and the National Institute of Standards and Technology.

The COVID-19 pandemic exacerbates the technical challenges election officials across the country face in preparing for secure, accurate elections this fall. We stand ready to assist you in securing the vote in whatever ways you and your staffs deem appropriate.

Thank you for all you do to preserve and protect our democracy.

Respectfully submitted,

Michael D. Fernandez, Founding Director  
Center for Scientific Evidence in Public Issues (EPI)  
American Association for the Advancement of  
Science

James Hendler, Chair  
U.S. Technology Policy Committee  
Association for Computing Machinery

Karen Hobert Flynn, President  
Common Cause

Ellen Zegura, Chair  
Computing Research Association

Paul Rosenzweig, Senior Fellow  
R St. Institute

John Bonifaz, President & Co-Founder  
Free Speech for People

Marian K. Schneider, President  
Verified Voting

## EXPERT ENDORSERS

Steven M. Bellovin, Hudson Prof. of Computer  
Science  
Columbia University  
Former Chief Technologist, U.S. Federal Trade  
Comm.  
Former Technology Scholar, U.S. Privacy and Civil  
Liberties Oversight Board  
Member, National Academy of Engineering

Vinton Cerf  
Internet Pioneer

Deborah Frincke  
Fellow, Association for Computing Machinery

Ronald L. Rivest, Institute Professor  
Massachusetts Institute of Technology  
Co-Creator, "RSA" Public Key Encryption Algorithm  
Assoc. for Computing Machinery A.M. Turing Award  
Fellow: American Academy of Arts & Sciences,  
Association for Computing Machinery  
International Assoc. for Cryptologic Research

Gene H. Spafford, Prof. and Exec. Director Emeritus  
CERIAS  
Purdue University  
Cyber Security Hall of Fame  
Distinguished Fellow: Info. Systems Security Assoc.  
Fellow: AAAS  
Association for Computing Machinery  
Inst. of Electrical and Electronics Engineers  
ISC<sup>2</sup>

Matthew Blaze  
McDevitt Chair of Computer Science and Law  
Georgetown University

Bruce W. McConnell, Executive Vice President  
EastWest Institute  
Former Deputy Under Secretary for  
Cybersecurity,  
U.S. Department of Homeland Security

Barbara B. Simons, Board of Advisors  
U.S. Election Assistance Commission  
Former President, Assoc. for Computing  
Machinery  
Board Chair, Verified Voting  
Fellow: AAAS  
Association for Computing Machinery

Daniel J. Weitzner, Founding Director  
Internet Policy Research Initiative  
Massachusetts Institute of Technology  
Former U.S. Deputy Chief Technology Officer  
Fellow, National Academy of Public  
Administration

April 9, 2020

Dear Governors, Secretaries of State and State Election Directors,

We are writing to share information on the scientific evidence regarding the security of internet voting. Based on scientific evidence, we have serious concerns about the security of voting via the internet or mobile apps.

The COVID-19 pandemic presents an unprecedented challenge to American elections. **At this time, internet voting is not a secure solution for voting in the United States, nor will it be in the foreseeable future.** Vote manipulation that could be undetected and numerous security vulnerabilities including potential denial of service attacks, malware intrusions, and mass privacy violations, remain possible in internet voting.

**We urge you to refrain from allowing the use of any internet voting system and consider expanding access to voting by mail and early voting to better maintain the security, accuracy, and voter protections essential for American elections in the face of an unprecedented public health crisis.**

**Internet voting is insecure.**

Internet voting, which includes email, fax, and web-based voting as well as voting via mobile apps such as Voatz, remains fundamentally insecure.<sup>1-10</sup> Scientists and security experts express concern regarding a number of potential vulnerabilities facing any internet voting platform, including malware and denial of service attacks; voter authentication; ballot protection and anonymization; and how disputed ballots are handled. Importantly, there is no way to conduct a valid audit of the results due to the lack of a meaningful voter-verified paper record. If a blockchain architecture is used, serious questions arise regarding what content is stored in it, how the blockchain is decrypted for public access, and how votes are ultimately transferred to some type of durable paper record.<sup>11</sup> **No scientific or technical evidence suggests that any internet voting system could or does address these concerns.**

A 2018 [consensus study report on election security](#) by the National Academies of Science, Engineering, and Medicine (NASEM), the most definitive and comprehensive report on the scientific evidence behind voting security in the U.S., stated:

“At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.”<sup>5</sup>

Federal researchers have also agreed that secure internet voting is not yet feasible.<sup>12</sup> The Department of Defense suspended an Internet voting trial after concluding it could not ensure the legitimacy of votes cast over the Internet<sup>13</sup> and the Pentagon has stated it does not endorse the electronic return of voted ballots.<sup>14</sup> Although the Department of Homeland Security has not published formal guidance on Internet voting, the Homeland Security cyber-division does not recommend the adoption of online voting for any

level of government<sup>14, 15</sup> Unlike most voting systems currently used in the United States, there are no standards for internet voting and no internet voting systems have been certified by the U.S. Election Assistance Commission.

### **Blockchain systems do not address the fundamental issues with internet voting.**

Blockchain-based voting systems introduce additional security vulnerabilities and do not address the fundamental security concerns scientists, election security experts, and government officials have expressed since the advent of internet voting.<sup>16</sup> **Rather than enhancing security, the 2018 NASEM report described the addition of blockchains to voting systems as “added points of attack for malicious actors.”**<sup>5</sup> Experts and researchers have expressed significant concern over the perceived security of blockchain technology,<sup>17</sup> more generally, but particularly regarding voting security.<sup>18, 19</sup>

MIT researchers reported a variety of potential vulnerabilities after examining a portion of Voatz code.<sup>20</sup> Researchers easily circumvented Voatz’s malware detection software, demonstrating a potential avenue to exposing the voter’s private information or manipulating their ballot. **Voatz’s servers are vulnerable to manipulation “surreptitiously violating user privacy, altering the user’s vote, and controlling the outcome of the election.”** Additionally, attackers could intercept a voter’s transmitted ballot prior to receipt by Voatz’s servers and determine how the voter voted because the information transmitted “clearly leaks which candidate was selected.”

Beyond potential ballot manipulation, Voatz potentially exposes a voter’s email, physical address, exact birth date, IP address, driver’s license or passport number, mobile phone number, a current photo of themselves, a short video of themselves, a copy of their written signature, their device’s model and OS version, and preferred language to third parties. **As a result, information captured from voters exposes them to serious risk of identity theft, and information from overseas military voters risks potentially providing adversaries with intelligence regarding military deployments, endangering the lives of service members and national security.**

An in-depth technical study from a private security group contracted by Voatz confirmed vulnerabilities previously reported by MIT researchers, despite the app developer arguing these vulnerabilities did not exist following the MIT report.<sup>21</sup> In total, the security group’s review highlighted seventy-nine findings with a third of the findings labeled as “high severity.”<sup>22</sup> Importantly, the review “did not even constitute the entire Voatz system, as the code for certain components such as the audit portal were never furnished,” indicating still undiscovered vulnerabilities and a lack of transparency essential for faith in the electoral system.<sup>23</sup>

### **Access to the ballot for all is an essential tenet of American democracy.**

At this difficult time, election officials seek to protect citizens’ health and access to the ballot. COVID-19 presents significant barriers to voting. However, internet voting is not a viable solution given the longstanding and critical security issues it presents. **Thoughtful implementation of alternative voting methods such as voting by mail and early voting can help support the diverse needs of the electorate, addressing both new concerns relating to COVID-19 and existing disparities in ballot access.**<sup>24-28</sup>

Incoming federal funding should help election officials implement alternative systems and offer increased flexibility to confront our ongoing challenges.<sup>29</sup>

Two decades of scientific and technical analysis demonstrate that secure internet voting systems are not possible now or in the immediate future. **In response to this evidence, we respectfully request that in your roles leading election security in your state, you refrain from allowing the use of any internet or voting app system.**

If we can provide additional scientific evidence regarding internet voting or do anything else to be a resource, please let us know. Our organizations and the scientists, engineers, and statisticians we represent stand ready to assist you.

Signed,

Barbara B. Simons, Board of Advisors, U.S. Election Assistance Commission

Andrew W. Appel, Professor of Computer Science, Princeton University

J. Alex Halderman, Director, Center for Computer Security and Society, University of Michigan

James Koppel, Ph.D. Candidate in Programming Languages, Massachusetts Institute of Technology

Bruce Schneier, Lecturer and Fellow, Harvard Kennedy School

Kevin Skoglund, President and Chief Technologist, Citizens for Better Elections\*

William Ramirez, Executive Director, ACLU PR/ACLU of Puerto Rico National Chapter\*

Michael A. Specter, Ph.D. Candidate in Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Dan S. Wallach, Professor of Computer Science, Rice University

Ellen Zegura, Chair, Computing Research Association\*

Free Speech for People

Edward W. Felten, Director, Center for Information Technology Policy, Princeton University

Mark Ritchie, Former Minnesota Secretary of State

Candice Hoke, Founding Co-Director, Center for Cybersecurity & Privacy Protection, Cleveland State University

John E. Savage, An Wang Professor Emeritus of Computer Science, Brown University

Eugene H. Spafford, Professor and Executive Director, Center for Education and Research in Information Assurance and Security, Purdue University

Douglas W. Jones, Associate Professor of Computer Science, University of Iowa

David L. Dill, Donald E. Knuth Professor Emeritus, School of Engineering, Stanford University

John L. McCarthy, Lawrence Berkeley National Laboratory (retired); Board of Advisors, Verified Voting

David Jefferson, Lawrence Livermore National Laboratory (retired); Board of Directors, Verified, Voting

Larry Diamond, Senior Fellow, Hoover Institution and Freeman Spogli Institute, Stanford University

Daniel J. Weitzner, Founding Director, Internet Policy Research Initiative, Massachusetts Institute of Technology

Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology

James Hendler, Director of the Institute for Data Exploration and Applications, Rensselaer Polytechnic Institute

Harry Hochheiser, Associate Professor, Department of Biomedical Informatics, University of Pittsburgh

Jeanna Neefe Matthews, Associate Professor, Department of Computer Science, Clarkson University

Deborah Frincke, Fellow, Association for Computing Machinery

Vinton Cerf, Internet Pioneer

Matthew Blaze, McDevitt Chair of Computer Science and Law, Georgetown University

Steven M. Bellovin, Percy K. and Vida L. W. Hudson Professor of Computer Science, Columbia University

Brian Dean, Privacy Subcommittee Chair, Association for Computing Machinery, U.S. Technology Policy Committee

Andrew Grosso, J.D., M.S. Comp. Sci., M.S. Physics, Andrew Grosso Associates

Steve M. Newell, Policy Director, Center for Scientific Evidence in Public Issues, AAAS

Michael D. Fernandez, Director, Center for Scientific Evidence in Public Issues, AAAS

Marian K. Schneider, President, Verified Voting

Ben Ptashnik, President, National Election Defense Coalition\*

Karen Hobert Flynn, President, Common Cause\*

Duncan Buell, NCR Professor of Computer Science and Engineering, University of South Carolina

David Mussington, Professor of the Practice and Director, Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland

Daniel M. Zimmerman, Principal Researcher, Galois

Paul Rosenzweig, Senior Fellow, R St. Institute

Richard Forno, Senior Lecturer and Director, UMBC Graduate Cybersecurity Program, UMBC

Kelley Misata, CEO and Founder, Sightline Security

O. Sami Saydjari, CEO, Cyber Defense Agency, Inc.

Matt Bishop, Professor of Computer Science, University of California at Davis

Patricia Youngblood Reyhan, Distinguished Professor of Law, Albany Law School

\*Signing on behalf of org

1. Greenhalgh, S.; Goodman, S.; Rosenzweig, P.; Epstein, J. with support from ACM Technology Policy Committee, National Election Defense Coalition, Common Cause and R Street Institute, Email and Internet Voting: the Overlooked Threat to Election Security, 2018.
2. Brandt, L. & Cheney, D., Internet Voting is no "Magic Ballot," Distinguished Committee Reports, Available at <https://www.nsf.gov/od/lpa/news/press/01/pr0118.htm> (2001).
3. U. S. Vote Foundation, The Future of Voting: End-to-End Verifiable Internet Voting, Available at <https://www.usvotefoundation.org/e2e-viv/> (2015).
4. Verified Voting, Computer Technologists' Statement on Internet Voting, Available at <https://www.verifiedvoting.org/wp-content/uploads/2012/09/InternetVotingStatement.pdf> (2008).
5. National Academies of Science, Engineering and Medicine, *Securing the Vote: Protecting American Democracy* (The National Academies Press, 2018).
6. California Secretary of State Bill Jones, Internet Voting Task Force, A Report on the Feasibility of Internet Voting, 2000.
7. Internet Policy Institute , Report of the National Workshop on Internet Voting Security, 2001.
8. Jefferson, D.; Rubin, A.; Simons, B.; Wagner, D., Analyzing Internet Voting Security. *Communications of the ACM* **47** (10) (2004).
9. Commission on Federal Election Reform, Building Confidence in U. S. Elections, 2005.
10. Simons, B.; Jones, D. W. , Internet Voting in the U.S. *Communications of the ACM* **55** (10), Available at <https://www.acm.org/binaries/content/assets/public-policy/jtreportemailinternetvoting.pdf> (2012).
11. Jefferson, D.; Buell, D.; Skoglund, K.; Kiniry, J.; Greenbaum, J., What We Don't Know About the Voatz "Blockchain" Internet Voting System, Available at [https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz\\_Blockchain\\_.pdf](https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf) (2019).
12. NIST Activities on UOCAVA Voting, Available at <https://www.nist.gov/itl/voting/nist-activities-uocava-voting>.
13. Garamone, J., Pentagon Decides Against Internet Voting this Year, Available at <https://archive.defense.gov/news/newsarticle.aspx?id=27362> (2004).
14. Gordon, G., As States Warm to Online Voting, Experts Warn of Trouble Ahead, Available at <http://www.mcclatchydc.com/news/politics-government/election/article24783181.html>. (2015).
15. Horwitz, S., More than 30 states offer online voting, but experts warn it isn't secure, Available at <https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/> (2016).
16. Park, S.; Specter, M.; Narula, N.; Rivest, R. L., Going from Bad to Worse: From Internet Voting to Blockchain Voting, Available at <https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf> (2020).



17. Alexandre, A., MIT Professor Asserts Blockchain Technology is Not as Secure as Claimed, Available at <https://cointelegraph.com/news/mit-professor-claims-blockchain-technology-is-not-as-secure-as-claimed> (2019).
18. Alexandre, A., MIT Professor: Blockchain is Good on Its Own, but Not Good for Voting, Available at <https://cointelegraph.com/news/mit-professor-blockchain-is-good-on-its-own-but-not-good-for-voting> (2020).
19. Juels, A.; Eyal, I.; Naor, O., Blockchain Won't Fix Internet Voting Security – And Could Make It Worse, Available at <https://www.govtech.com/security/Blockchain-Wont-Fix-Internet-Voting-Security--And-Could-Make-It-Worse.html> (2018).
20. Specter, M. A.; Koppel, J.; Weitnzer, D. , The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections, Available at [https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz\\_Public.pdf](https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf) (2020).
21. Trail of Bits, Available at <https://www.trailofbits.com/about/> (2020).
22. Edwards, S.; Smith, J.P.; Guido, D.; Sultanik, E., Voatz, Security Assessment I of II: Technical Findings, Available at <https://github.com/trailofbits/publications/blob/master/reviews/voatz-securityreview.pdf> (2020).
23. Trail of Bits, Our Full Report on the Voatz Mobile Voting Platform, Available at <https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/> (2020).
24. Misra, J., Voter Turnout Rates Among All Voting Age and Major Racial and Ethnic Groups Were Higher Than in 2014, Available at <https://www.census.gov/library/stories/2019/04/behind-2018-united-states-midterm-election-turnout.html> (2019).
25. Rutgers School of Management and Labor Relations, Report: Voter Turnout Surges Among People with Disabilities, Available at <https://smlr.rutgers.edu/news/voter-turnout-surges-among-people-disabilities> (2019).
26. Weiser, W. R.; Feldman, M., How to Protect the 2020 Vote from the Coronavirus, Available at <https://www.brennancenter.org/our-work/policy-solutions/how-protect-2020-vote-coronavirus> (2020).
27. National Task Force on Election Crises, COVID-19 Election Guide, Available at [https://static1.squarespace.com/static/5e70e52c7c72720ed714313f/t/5e7ba6fc6ec60c0341aa7d2d/1585161982796/COVID-19+Election+Guide+-+FINAL+Draft+3\\_25\\_20+%281%29.pdf](https://static1.squarespace.com/static/5e70e52c7c72720ed714313f/t/5e7ba6fc6ec60c0341aa7d2d/1585161982796/COVID-19+Election+Guide+-+FINAL+Draft+3_25_20+%281%29.pdf) (2020).
28. Stewart, C., Will Expanded Early Voting Help with Social Distancing? Maybe Not, Available at <https://electionupdates.caltech.edu/2020/03/25/will-expanded-early-voting-help-with-social-distancing-maybe-not/> (2020).
29. Miller, M., Senate includes \$400M for mail-in voting in coronavirus spending deal, Available at <https://thehill.com/policy/cybersecurity/489435-senate-includes-400-million-for-mail-in-voting-in-coronavirus-spending> (2020).