Leveraging Electronic Balloting Options Safely and Securely During the COVID-19 Pandemic

JUNE 2020

Susan Greenhalgh
Free Speech For People

Steve Newell, Ph.D., M.M.Sc.
American Association for the Advancement of Science,
Center for Scientific Evidence in Public Issues

INTRODUCTION

As States grapple with the difficult task of holding elections during the novel coronavirus pandemic, election administrators are exploring and implementing technology to enhance capacity to deliver blank ballots electronically. The expansion of vote by mail in many states necessitates a remote accessible ballot marking option for voters with disabilities. This paper examines these procedures and available technologies, and offers specific recommendations to limit the security and privacy risks introduced with electronic blank ballot delivery and remote electronic ballot marking.

The most secure option for remote voting is to mail pre-printed paper ballots to voters, as is traditionally done for mail-in ballots. This allows ballots to be hand-marked and to be mailed back or dropped off in a condition suitable for immediate scanning, eliminating the need to re-make the ballot. Jurisdictions should make every effort to ramp up their capability to bulk mail paper ballots to all voters, or to as many as allowed by law.

In jurisdictions unable to procure sufficient pre-printed ballots, officials should explore options for providing blank ballots through the Internet. Most voters would then print the blank ballot on their own printers, mark their choices with a pen, and mail it back. Voters who can mark a ballot privately and independently by hand should be advised not to mark the ballot electronically before printing, even if that capability is available in the software they are using. Electronically delivered ballots pose a higher risk of unauthorized duplication, warranting authentication of the voter's identity and eligibility.

Only voters with a disability impacting their ability to mark a ballot by hand should have access to remote electronic ballot marking systems. The most secure systems for remote accessible ballot marking confine vote selection data to the voter's devices, are not connected to the Internet when selections are made, and remove vote choices from all memory upon closing. See detailed recommendations on page 6.

1. Remote Accessible Ballot Marking

Providing Remote Accessible Ballot Marking that Protects Privacy and Security

As states expand vote by mail in response to the novel coronavirus pandemic, it is imperative that they provide voters that may be unable or uncomfortable hand-marking a paper ballot an option for secure, private and accessible marking of a ballot for printing and mailing. States are facing legal challenges from disability rights organizations demanding a remote accessible option. Remote ballot marking should conform to security and privacy best practices that do not transmit vote choices or voted ballots over the internet.

There is broad scientific consensus that voted ballots transmitted over the internet are not secure. A 2018 consensus study report on election security by the National Academies of Science, Engineering, and Medicine (NASEM) stated that "no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet." Recently,

the Department of Homeland Security, FBI and other federal agencies distributed a threat assessment that strongly warns that ballots returned over the internet are at high risk of compromise and manipulation.

Selecting a Remote Accessible Ballot Marking System that Protects Voters' Privacy and Security

A number of available systems allow the voter to receive a blank ballot electronically, mark it on their computer and print it for mailing or drop off without transmitting the voted ballot to the election office. However, these remote accessible ballot marking systems can be designed in two different ways that have significantly different security and privacy profiles.

More secure, *offline* systems are designed so that once the ballot is accessed on the voter's computer, the ballot and vote selection data reside on the voter's computer during the entire marking, ballot rendering and printing process. Systems of this design allow voters to access and mark a ballot on their own computers with assistive technology without exposing the voter or the ballot to unnecessary online privacy and cyber security risks. These systems are designed to conduct the marking process offline while providing full ballot accessibility. There are several commercially available systems which meet this design standard.

Less secure, *online* systems access the ballot information on a remote server run by the vendor or state or county and maintains an active internet connection during the entire marking process. As the voter makes selections, those selections are transmitted over the internet and recorded on the remote server. When the voter has completed the ballot marking process, the remote server then renders the ballot to a printable PDF form and that PDF is sent over the Internet back to the voter's computer for printing and mailing or drop off.

Maryland's ballot distribution system (also adopted in New Mexico) and many of the commercially available options operate as less secure, online systems and routinely transmit voters' choices back and forth via the Internet as the ballot is marked and formatted for printing by the voter. In some systems the vote choices are stored as the voters marks their ballots in a file that also contains the voter's identity, enabling a wholesale voter privacy violation by the state and any other actors who gain access to the system.

The National Institute of Standards and Technology (NIST) researched this topic and advised that online remote ballot marking systems are vulnerable to online cyberattacks and privacy violations. NIST further recommends that all remote ballot marking should run solely on the voter's computer, offline.

> "*To protect ballot secrecy, the printable ballot should be constructed using software that runs solely on voters' computers. At no point should the ballot marking application transmit voter selections to the Web-server."* – NIST IR 7711

The Center for Civic Design (CCD) made a similar recommendation in its report "Principles and Guidelines for Remote Accessible Ballot Marking" because transmission of the vote selections

over the Internet during the remote marking process, even if the voter prints the ballot and mails it in, will expose the ballot to significant privacy and security threats.

> *"The system should not transmit vote choices to a remote server in order to mark and print ballot. To safeguard privacy and security, any communication function should be disconnected or disabled while marking the ballot. This applies to functions of the system."* – Principles and Guidelines for Remote Accessible Ballot Marking.

Dr. Juan Gilbert, a noted computer science professor who has studied voting system accessibility and security, reiterated the importance of ensuring remote accessible ballot marking be done offline at the May 6, 2020 U.S Election Assistance Commission hearing.[1]

It is a misconception that remote accessible ballot marking must be conducted *online* with an active connection to the Internet. Online systems that transmit the choices over the internet needlessly expose the voted ballot to security and privacy attacks. Voters with disabilities should not have to settle for insecure voting methods when more secure alternatives are available.

We urge all states to adopt an ***offline*** accessible remote ballot marking system to ensure all voters who require an accessible remote ballot marking system to vote can cast absentee ballots privately and independently.

California Bans Accessible Marking on Remote Servers

When California was transitioning to mostly vote-by-mail, the State recognized the necessity of providing a remote accessible ballot marking option. Mindful of the security and privacy risks associated with systems that transmit vote choices to a remote server, the legislature passed AB1929 in 2012 prohibiting remote ballot marking systems that transmit vote selections to remote server. California has certified three systems which meet this requirement: Democracy Live Secure Select 1.2.2, Five Cedars Group Alternate Format Ballot (AFB) v5.2.1 and Dominion ImageCast Remote 5.2.

Maximizing Security when Using Remote Accessible Ballot Marking Systems

Protecting remotely marked ballots from cyber security threats to the integrity of ballot: If the voter's device is infected with malware, or the marking or printing application is simply buggy, it may record false votes on the printed ballot. Just as with a precinct-based ballot marking device (BMD) this leaves the voter with the task of carefully verifying that the printed ballot correctly reflects his or her intentions. Election officials should provide clear guidance to voters with disabilities that it is critical to perform this verification step.

[1] *Available at: https://us02web.zoom.us/rec/play/uJIsIu2t_zM3SICcsASDBfJ_W47vLf2shCYX_KUJmE60UiZWNQD3MrYWZeWiE7RxmpQBOKeryyTXeY27 at 1:28:30*

***Protecting the secrecy of ballots marked remotely*:** If the voter enters their vote choices into their computer or mobile device, the secrecy of the votes is at risk even if the system marks votes offline. Copies of the votes will still remain in the clear in the device's RAM and virtual memory unless the application has been carefully designed to zero that data before the application is closed. Images of the voted ballot will also remain as invisible temporary files in the device's file system and in the file system and memory of the printer or print server, at least until they are overwritten or intentionally deleted by the application, meaning the votes are available to any skilled person for a substantial time after voting is complete. We urge states and election officials not purchase or certify client applications unless they are verified to perform this deletion step when the application is closed.

Avoiding networked or public device for marking ballots: Data sent to a networked printer is generally transmitted in the clear, so any other computer on the same network can monitor the network traffic and make a copy of the voted ballot being printed, compromising vote secrecy.

A voter who uses a business-, institutional- or employer-owned device or network or printer may have no right of privacy. All three may be freely monitored without the voter's knowledge or consent. Voters who must input their votes electronically should use their own personal devices, networks, and printers if possible, unless the voter is concerned about privacy in their home environment.

Barcodes and QR codes: The need for voter verification of machine-marked ballots is critical. Some marking systems record vote selections in human-readable text and in a barcode enabling the ballot to be scanned for remaking or counting. The use of a barcode introduces additional layer of digital vote data which could be incorrectly recorded but cannot be verified or corrected by the voter. States and localities are discouraged from enabling the barcode feature and encouraged to count or remake ballots from the human-readable text selections. Since barcodes and QR codes will not be printed on hand-marked ballots, leaving them off of machine-marked ballots has the positive advantage of making them harder to distinguish from the hand-marked ballots. If they choose to use the barcode feature, election administrators are encouraged to instruct poll workers remaking the ballots to carefully check each ballot to ensure the remade ballot matches the human-readable selections on the original ballot. The original ballot should be retained and used in audits and recounts.

2. Minimizing Risks with Online Blank Ballot Delivery

Online transmission of *blank* ballots does not have the same risk profile as the electronic transmission of *voted* ballots but there are several risk factors that warrant strict limitations of online blank ballot delivery wherever possible.

Threats to the integrity and security of blank ballots delivered online: Transmitting a blank ballot to a voter for printing and hand-marking raises a number of standard cybersecurity concerns because the ballot server must be online, exposing it to online attackers that could corrupt the ballot files sent to the voters. Offering unlimited or large-scale online ballot delivery will make electronically delivered ballots an attractive hacking target. Contests and/or

candidates could be deleted, rearranged, or altered by a motivated hacker to corrupt an election contest. Some voters might notice that they did not receive the correct contests or candidates on their ballots, but there remains a serious risk that voters will not notice it. Even if a voter does notice an error, it may be difficult to alert election officials in a timely way so that the error can be discovered and corrected for all affected voters.

Online blank ballot delivery may provide opportunities to cast fraudulent ballots: By impersonating legitimate voters, online blank ballot delivery may be exploited by criminals or hackers anywhere in the world. Attackers could also intercept emails sent to voters that requested blank ballots and vote their absentee ballots. Verification of voters' signatures on submitted ballots (which has shortcomings) may be the only barrier to fraud, and not every state requires verification of the voters' signatures. Though some states require digital personal identifying information (partial social security number, date of birth, driver's license number, etc.) as credentials to request an absentee ballot, that information is typically easily available for tens of millions of voters due to previous mass breaches of online databases, potentially allowing an attacker to impersonate voters and successfully request and cast fraudulent absentee ballots if there is no signature check on the mailed-in ballot envelope.

The U.S. Senate Intelligence Committee Report on Foreign Interference warned of ongoing collection of information routinely used to validate a voter's absentee ballot request including voters' email addresses by Russian agents.[2] Bad actors can use voters' credentials to:

- Register eligible citizens that are not registered to vote, and then download and vote their absentee ballots.
- Request absentee ballots on behalf of registered voters and ask the ballot be delivered to an email address owned by the attacker.
- Print multiple copies of a ballot in order to cast fraudulent ballots. (This attack could be defeated by requiring signature verification for the submitted ballot but this practice is not universal. For example, Maryland has adopted online ballot delivery, but validates voters only at the ballot request stage. There is no voter authentication step when the ballot is received and counted.)

Many of these attacks could be partly or wholly, automated, making the attacks easier to scale and much more dangerous.

Remaking of ballots printed by voters burdens election workers, introduces opportunities for error or fraud and may increase the health risks to election workers: Many ballot scanners cannot read ballots printed from voters' home printers because the paper weight and size is incompatible, so the voter's selections must be laboriously hand-copied onto traditional paper ballot stock that can be read by a scanner. This is a time and resource-consuming process that may create a health risk for election workers who are typically directed to sit in pairs in order to prevent manipulation or fraud. Without transparent oversight and strict security protocols, this process introduces opportunities for error or tampering.

[2] Excerpts from an alleged leaked NSA document indicate that the hackers might have been exploring vulnerabilities associated with online delivery of absentee ballots. The top of the leaked document says: "*Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors...Research Absentee Ballot email addresses.*"

When remaking ballots, jurisdictions should be advised to retain the original ballots and use them (rather than the remade ballots) for audits and recounts.

The best way to mitigate these risks is to minimize the reliance on the online delivery of blank ballots as much as possible by maximizing the ability to provide pre-printed paper absentee ballots to voters.

Recommendations:

- Only adopt and certify remote accessible ballot marking systems that confine vote selection data to the voter's devices and remove vote choices from all memory upon closing.
- Place limits on electronic ballot delivery, provide only to those who cannot be mailed a pre-printed blank ballot, who are required to have electronic delivery available by law, or who have disabilities that impact the voter's ability to hand-mark a ballot.
- Make *printing the blank ballot* the default action of any ballot download application, and encourage all voters who are able to do so to fill out the printed blank ballot with a pen before mailing.
- Advise voters who must input their votes electronically to use their own personal devices, networks, and printers, if possible, rather than an employer's or institution's infrastructure, unless they are concerned about privacy at home.
- Recommend clearly that no voter should ever enter enter choices into any device while it is connected to the Internet.
- Instruct voters who do mark their ballots with a computer or device application to carefully verify that their vote choices were recorded correctly.
- Disable the barcode feature on accessible ballot marking systems and remake ballots directly from the voters' selections.
- Retain the original ballots and use the human readable portion (rather than the remade ballots, barcodes, or QR codes) for audits and recounts.
- Consider electronically delivered ballots to be at higher risk of unauthorized duplication, warranting authentication of the voter's identity and eligibility.

ABOUT THE AUTHORS

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from The New York Times, The Washington Post, The Wall Street Journal, Politico, USA Today, Associated Press, National Public Radio and other leading news outlets. She has appeared on CNN and MSNBC's The Rachel Maddow Show, and various other television news shows. She has a BA in Chemistry from the University of Vermont.

Dr. Steve Newell is a project director at the Center for Scientific Evidence in Public Issues (EPI Center). Prior to joining AAAS, he was a Senior Legislative and Federal Affairs Officer at the American Psychological Association, where he promoted evidence-based policy and federal investments in science.

Dr. Newell was an AAAS Science and Technology Policy fellow from 2015 to 2016 with the office of Senator Bernie Sanders (I-VT) and the National Institute on Minority Health and Health Disparities from 2016 to 2017. He received his bachelor's degree in psychology from the University of North Carolina at Chapel Hill, and a masters in Medical Science, with a concentration in Health Outcomes and Policy, and Ph.D. in Social Psychology from the University of Florida.

ABOUT FREE SPEECH FOR PEOPLE

Free Speech For People works to renew our democracy and our United States Constitution for we the people. Founded on the day of the Supreme Court's *Citizens United* ruling, Free Speech For People envisions a democratic process in which all people have an equal voice and an equal vote. We fight for free and fair elections, for reliable and secure voting systems, and for the bedrock principle that, in a democracy, all voters must have their votes properly counted. To learn more, please visit our website: www.freespeechforpeople.org.

ABOUT THE AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE (AAAS), CENTER FOR SCIENTIFIC EVIDENCE IN PUBLIC ISSUES

The American Association for the Advancement of Science (AAAS) seeks to advance science, engineering, and innovation throughout the world for the benefit of all people. The AAAS EPI Center is designed to provide scientific evidence to policymakers and other decision-makers in ways that are clear, concise, and actionable. We make it easier for people to access scientific evidence and information and then integrate that evidence into their decision-making process. To learn more, please visit: www.aaas.org/epicenter.