House Bill 0955
Election Law – Absentee Ballot Delivery and Marking
SUPPORT

Ways and Means

February 16, 2021

Poorvi L. Vora
Professor of Computer Science, The George Washington University

Maryland's approach to internet ballot delivery is unintentionally, yet fundamentally, flawed and among the most insecure in the nation. The change implemented in HB 0955—restriction of the use of online ballot delivery—is urgently needed. In the absence of this restriction, Maryland opens itself to a variety of disruptions as the number of voters using online ballot delivery increases. Some of these disruptions could create far greater chaos than was witnessed last year in the Iowa caucuses[1]. Maryland should make every effort to limit the use of online ballot delivery to those voters needing it.

Computer scientists have written to the Maryland State Board of Elections regarding internet ballot delivery since 2012; I have personally written and testified four times[2]. The SBE's overconfidence and disregard of our recommendations only increases its attractiveness as a target. It is very easy for a bad actor to obtain thousands of voting credentials and request and complete thousands of online ballots from anywhere in the world. It is then trivial to have these ballots mailed in from within the US, and the State would not be able to distinguish fraudulent ballots from those completed by real absentee voters. If voters were to arrive to vote on Election Day and were told absentee ballots were requested on their behalf, there would be significant disruption. The incentive for bad actors to exploit this vulnerability, and the extent of the disruption, will increase with the number of voters using online ballot delivery.

---

[1] Reid J. Epstein, Sydney Ember, Trip Gabriel and Mike Baker, "How the Iowa Caucuses Became an Epic Fiasco for Democrats", New York Times, Published Feb. 9, 2020. Updated Feb. 11, 2020. https://www.nytimes.com/2020/02/09/us/politics/iowa-democratic-caucuses.html as accessed on February 11, 2021.

[2] I wrote a letter, with others, to the SBE and several legislators on 15 January 2018 and another letter earlier to the SBE on 12 September 2016. I testified in person at the hearings for HB 0859, HB 706 and HB 1658 on 18 February 2020, 26 February 2019 and 27 February 2018 respectively, and earlier at a State Board meeting on 14 September 2016. Other computer scientists have sent letters earlier.

A simple measure would greatly reduce Maryland's vulnerability and HB 0955 implements it by restricting the use of online ballot delivery. All other voters could still request their ballots using the online ballot request tool. Reducing the number of electronically-delivered ballots would reduce both the incentive for bad actors and the likelihood of significant chaos through fake absentee ballots.

Security technology alone cannot adequately address the possible acceptance of fraudulent ballots made easy by the use of intermediating computers, weak authentication, stolen credentials, emailed ballot links and insecure computers used by voters. As more voters use the online ballot delivery system, the State becomes a more attractive target. Further, in spite of a best practice requirement that signatures be used as the primary authentication mechanism for voted absentee ballots (see NIST IR 7711[3]), Maryland does not compare voter signatures for returned voted ballots. Electronically-delivered ballots are delivered as internet links to email accounts; it is comparatively easy to set up fake email addresses in bulk. Hence, unlike ballots obtained at brick-and-mortar addresses or voted in person, electronically-delivered ballots may be obtained and cast in large numbers by bad actors. The bad actor may be a nation state, or any domestic or international group or individual.

Maryland's legislators have the charge to greatly reduce the possibility of disruption of Maryland's elections by passing this Bill. I understand and applaud the desire to improve voter services, but all voters suffer when elections are interfered with. **I urge you to pass this Bill.**

Respectfully,

Prof. Poorvi L. Vora

Professor of Computer Science
The George Washington University, DC
Note: affiliations are included for identification only

Poorvi L. Vora is Professor of Computer Science at The George Washington University. Her research focus has been on end-to-end independently verifiable (E2E) voting systems and statistical election audits. She has worked with the National Institute of Standards and Technology (NIST) on definitions of desired properties of E2E systems, and on information--theoretic models and measures of voting system security properties. She obtained her Ph.D. from North Carolina State University.

poorvi@gwu.edu

[3]"In most cases, any mechanism used to remotely authenticate voters will serve as a secondary method to authenticate returned ballots, with voter signatures generally providing the primary mechanism to authenticate returned ballots." NIST IR 7711, Sept 2011, "Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters".

APPENDIX A: Disrupting an Election Using Online Ballot Delivery

A bad actor can easily obtain access to voter registration lists, voting records and the personal information required to register voters and/or request online absentee ballots. Thousands of online ballots can be obtained in one of many ways (some are listed below). The bad actor, using registered voters' credentials, downloads the online ballots, completes them through computerized ballot marking and prints them. All of this can be easily automated by software written for the purpose. The completed fake ballots would be mailed by humans. If, as a consequence, Maryland's counties received multiple ballots for many voters, they would have no way of distinguishing legitimate absentee ballots from fake ones, because *Maryland does not compare signatures for absentee ballots.*

Fraudulent Means of Access to Online Ballots

1. **Use credentials to impersonate registered voters who vote regularly and create chaos on Election Day**

Using the credentials for voters who vote regularly, the bad actor creates many thousands of fake email addresses, and then makes thousands of fake online absentee ballot requests to be sent to fake email addresses. All of this can be automated through software written for this purpose, and need not be done manually. Most of these voters will show up to vote on Election Day and will need to complete provisional ballots, which will create a great deal of chaos and distrust at the polls. By Maryland election law[4], if an absentee ballot has been received for this voter, both ballots will be rejected. If a voter does not show up to vote, neither they nor the State will know that a fraudulent vote was cast on their behalf.

2. **Use credentials to impersonate registered voters who vote infrequently and attempt to change the election outcome of a primary election**

Using the voter registration list and the credentials of voters who do not vote often in primaries, the bad actor would request internet delivered ballots by impersonating these voters and then complete and mail voted ballots. This could change the outcome of the primary. Some voters may show up to vote and would cast provisional ballots, but most will not and will not know a vote was cast on their behalf.

---

[4] COMAR: 33.11.05.04
.04 Ballot Rejection — Multiple Ballots from the Same Individual.
C. If an absentee ballot and provisional ballot are received from the same individual, the local board shall reject both ballots.

3. Send incorrect links to voters

Voters who have requested an internet delivered ballot in the past can be sent incorrect links by the bad actor, spoofing the local election board. Voters might follow instructions on what they believe to be a state website. They would then download their ballot from the fake website and mail it to the given address. Even if the given address were correct, their ballot would not be counted because they had never officially requested a ballot. Yet they would believe they had voted. There have been reports[5] that Russian actors explored the possibility of spoofing state election email accounts in 2016, though any such accounts were probably not used in 2016.

Impact on the voters who are impersonated by the software

a. Real voters showing up at the polls on Election Day will need to cast provisional ballots.
b. Voters who did not request absentee ballots and did not vote won't know that a vote was cast on their behalf.
c. Voters who did request and cast absentee ballots could have their vote replaced if the fake ballot is received after theirs. They too would not know their vote was replaced. If there were many instances of multiple ballots being received for a single voter, the state would investigate, however this would not be easy to resolve without contacting each voter and causing chaos and distrust.

The State cannot do much if fraud is suspected.

a. The State cannot distinguish between legitimate returned absentee ballots and fake ones.
b. The State cannot reassure real voters who voted with an absentee ballot obtained online that a fake ballot was not received after their legitimate ballot and counted instead. If two ballots were received, ostensibly from the same voter, the State may not be able to tell which one was genuine, especially without an intensive investigation.
c. The State will find it hard to reassure those voters who did not vote that a vote was not cast on their behalf. There will be considerable difficulty if a voter claims they did not cast a vote, but the State has a vote ostensibly completed by the voter, which is counted.
d. Moreover, a bad actor can create long lines and chaos at the polls merely by fraudulently requesting an online ballot, without having to vote and return those ballots. At the polls, the e-poll books will record that an absentee ballot has been requested and sent; and that annotation alone will require that the voter vote a provisional ballot.

[5] https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1 pg. 4

APPENDIX B: The Context

Foreign actors, thought to be Russians, attempted to breach online voter registration databases throughout the US in 2016, and the FBI found that they were successful in doing so in at least one state. Additionally, thousands of fake social media accounts were created and successfully created and operated. While the state of Maryland detected attempts to breach its online voter registration database, officials have testified that they believe the attempts were not successful. But it is not possible to categorically state that a security breach did not occur, because it is relatively easy for competent attackers to hide their trail. Large organizations with considerable resources have been subject to data breaches. (Examples include Equifax, the US Government's Office of Personnel Management, Adobe, Sony, Capital One, Yahoo, Target, Marriott, the University of Maryland, Anthem Health Insurance). It typically takes many months for an organization that does not immediately detect a breach to become aware of it. There are likely many organizations that are successfully breached but never detect the breach.

Any online voter registration database, including Maryland's, can be breached, and it is likely to be a while before the breach is discovered, if ever. Additionally, some attacks do not require the hacking of Maryland's election technology. For example, as with social media accounts, the creation of fake email accounts in bulk is very easy.

The Ease of Obtaining Credentials

The personal information required to request and download an absentee ballot in Maryland (such as driver's license number or birth date) is no longer sufficiently confidential for voter authentication.

- All the information is easily available on the "dark" market—consider the description, in the Mueller indictment of 16 February, of Russians using the social security numbers of real US citizens in order to open bank accounts[6].
- It is also shared legitimately and widely among law enforcement agencies, universities, doctors' offices and hospitals, and hence could be leaked (or may already have been) through data breaches of these entities.

[6]"In or around 2016, Defendants and their co-conspirators also used, possessed, and transferred, without lawful authority, the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent. Using these means of identification, Defendants and their co-conspirators opened accounts at PayPal, a digital payment service provider; created false means of identification, including fake driver's licenses; and posted on ORGANIZATION-controlled social media accounts using the identities of these U.S. victims. Defendants and their co-conspirators also obtained, and attempted to obtain, false identification documents to use as proof of identity in connection with maintaining accounts and purchasing advertisements on social media sites", page 16, para 41, *ibid*.

- Additionally, the recent hacks of credit agency Equifax and the federal Office of Personnel Management (OPM) revealed considerably more "secure" information on a huge number of US voters and are believed to have been carried out by a state actor. Because this information is not yet on the "dark" market for personal gain, it is suspected to have been obtained for some other purpose appropriate for a state actor.
- Finally, ByteGrid servers stored the credentials of all Maryland voters, and an interested ByteGrid insider could have obtained access to all the credentials without leaving a trail.

In fact, reliance on personal data alone to authenticate a voter is never sufficient for any high security activity like voting, and changing the type of data required will not solve this problem.

The Ease of Obtaining and Completing Ballots in Bulk

It is not hard to automate access, download and completion of online ballots. The Mueller indictments describe how Russian trolls from a single company opened and ran hundreds of email and social media accounts[7], pretending to be US citizens. The company's annual expenditure was in the millions of dollars[8].

- "Tests" to differentiate humans from software are not very effective—consider that the Russians are believed to have created many thousands of fake social media accounts that are operated by software, behave like human participants, and exist solely for the purpose of interfering in the US election.
- It is also easy to make fake ballot requests appear to come from different IP addresses, spaced out over time, with an extremely large number being made close to deadlines, making it harder to detect them or respond effectively.
- The Mueller indictment describes how Virtual Private Networks (VPNs) and computer infrastructure in the US[9] were used to disguise the computers and the location of those opening and using the accounts.

The Ease of Casting Illegitimate Ballots in Bulk with Online Ballot Delivery

Bulk impersonation attacks have not been detected in Maryland in the past. However, a determined actor could easily obtain bulk access to virtual ballots delivered online.

---

[7] "Defendants and their co-conspirators also registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups", pg. 16, para 40, *ibid*.

[8] "The ORGANIZATION [Internet Research Agency] employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The ORGANIZATION's annual budget totaled the equivalent of millions of U.S. dollars", page 5, para 10(a), *ibid*.

[9] "Defendants also procured and used computer infrastructure, based partly in the United States, to hide the Russian origin of their activities and to avoid detection by U.S. regulators and law enforcement", page 3, para 5, *ibid*.

Information on who votes regularly and who does not is also easily available; to create chaos on Election Day, an adversary would focus attention on those who do vote often. To prevent fraudulently-obtained ballots from being cast, and in order to ensure that a voted ballot received by the election authority was indeed sent by the voter, the State should check signatures, which it does not. There is no way of determining whether a received, voted absentee ballot was indeed cast by the voter.

Potential Impact

If many voters show up to vote on Election Day but have absentee ballots cast in their names, it will take a while to determine what the correct election outcome is. Voters not paying much attention to their mail might find out on Election Day that the State received a change of address on their behalf and believes they live elsewhere; hence they are not eligible to vote in the jurisdiction they live in. If provisional ballots are cast, these will not be tallied toward the outcome announced on the evening of Election Day. Additionally, election officials would then be hard pressed to explain why they ignored several letters from computer scientists urging them to address the core problem. This could easily surpass the problem faced by the Democratic Party in Iowa.