House Bill 706
Election Law – Absentee Ballot Requests, Delivery, and Marking
SUPPORT

Ways and Means
February 26, 2019

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

Maryland's approach to electronic ballot delivery is unintentionally, yet fundamentally, flawed. The flaws jeopardize both ballot secrecy and election integrity and cannot be addressed by securing the SBE server. The change implemented in HB 706—restriction of the use of online ballot delivery—is urgently needed.

Computer scientists have been writing to the Maryland State Board of Elections regarding this and related issues since 2012; I have personally written and testified twice[1]. Suspected Russian interference in 2016, the Russian interest in ByteGrid, and the information released by Special Counsel Mueller in indictments[2] has added a great deal of urgency to our concerns. Maryland is an attractive target because a bad actor can tamper with its elections without hacking into any part of its election technology. Our intelligence agencies advise that Russian efforts to interfere in our elections will increase in intensity over time, and the interest in Maryland's servers and in ByteGrid appear very much like tests to assess its readiness to protect its elections. The state's blithe ignorance of our recommendations only increases its attractiveness as a target. In the event that this Bill does not pass, legislators should ask themselves how they would respond should the upcoming election be disrupted.

Maryland's well-intentioned efforts to secure its software and server can, at best, protect the information and votes it holds from future breaches.

- *The conclusion of the NCCIC report that it "did not positively identify any threat actor activity on … ByteGrid" relates only to outsider attacks, by entities other than those with authorized access to ByteGrid systems. The report does not provide any reassurance that a ByteGrid insider did not obtain and make a copy of the voter credentials stored on its servers before Maryland discontinued its services.*

[1] 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 hearing for HB 1658 on 27 February 2018, and earlier at a State Board meeting on 14 September 2016. Other computer scientists have sent letters earlier.
[2] U.S. v. Internet Research Agency, et al (1:18-cr-32, District of Columbia), 16 February, 2018. https://www.justice.gov/file/1035477/download

- *The State cannot address with security technology the entry of fraudulent votes 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.*

Maryland is among only three states that allow all voters to receive blank ballots online. However, 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]), the State does not check voter signatures on returned voted ballots. This makes it easy for a bad actor to illegitimately obtain and cast electronic ballots in bulk. The bad actor may be a nation state, or any domestic or international group or individual. Electronically-delivered ballots are delivered as internet links to email accounts; it is comparatively easy to set up fake email addresses in bulk. Paper ballots, on the other hand, are delivered to physical addresses; fake physical addresses are substantially harder to create in bulk.

A simple measure would greatly reduce Maryland's vulnerability and HB 706 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 probability of significant election fraud through fake absentee ballots.

The Process of Interfering in an Election

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 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. These ballots would be accepted and counted as legitimate because Maryland's counties have no way of distinguishing legitimate absentee ballots from fake ones, because *Maryland does not check signatures on absentee ballots!*

Fraudulent Means of Access to Online Ballots

1. Use credentials to impersonate registered voters 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. Most of these voters will show up to vote on Election Day and will

[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".

need to complete provisional ballots, which will create a great deal of chaos and distrust. 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 and attempt to change the election outcome of a primary election**

Using the credentials of voters who do not vote often in primaries, the bad actor would obtain, 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.

3. **Use credentials to impersonate unregistered voters, register them, request and vote online ballots**

When the voter is registered, a postcard may be sent to the original address, and a voter may notice it, but not many are likely to draw the State Board's attention to this. Most will not know a ballot was cast on their behalf.

4. **Send incorrect links to voters**

Voters can be sent incorrect links by the bad actor, spoofing the local election board, and might follow instructions on what they believe to be a state website, giving up valuable information in the process. They would believe they mailed in a ballot to the state when they did not; the information they divulged could be used to obtain and vote ballots on their behalf. There have been reports that Russian actors explored the possibility of spoofing state election email accounts in 2016, though any such accounts were probably not used.

5. **Hack into voter email accounts**

This provides one more means to harvest absentee ballots. If the bad actor waits till very late to mail in their ballots, these will replace any ballots cast by the voter.

6. **Write malware for voters' computers to obtain their online ballots**

The malware would access the ballot when the voter downloads it, complete the ballot, and secretly transmit the now voted ballot over the internet to the bad actor's server. The voter, who is unaware of the attack, might also complete and mail the ballot. Their vote would be replaced if the fake ballot is received after theirs. They would not know their vote was replaced.

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.

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 cannot tell which one was genuine.

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.

Voters can be targeted, based on the desired outcome.

a. If the bad actor wishes to **create chaos**, it would target those who vote often. In addition to being **terrible publicity** for the state, this would also **call into question a legitimate outcome**.

b. If the bad actor wishes to **change the election outcome without detection**, it would target unregistered voters and those who vote infrequently. Registering voters online is also easy, and the phony new registrations would be useful for subsequent election fraud.

In the event that the Bill does not pass, and any of the above takes place, how will the Legislature and the SBE explain why they ignored repeated warnings from computer scientists?

We understand and applaud the desire to improve voter services, but all voters suffer when elections are interfered with. **We urge you to pass this Bill.**

Respectfully,

Prof. Poorvi L. Vora
Professor, Department 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. She was a member of the team that deployed E2E voting system Scantegrity II in the Takoma Park elections of 2009 and 2011. 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

APPENDIX

The Context

As mentioned in the main body of this letter, computer scientists have been writing to the State Board of Elections regarding this issue since 2012. Most recently, in 2016, one of us also presented these concerns in person at an SBE meeting. Since then, it has been reported that US intelligence agencies believe Russia attempted to interfere in the 2016 elections, and its efforts are expected to increase in intensity and capability in future elections.

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, Yahoo, 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[4].

[4]"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

- 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.
- 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[5], pretending to be US citizens. The company's annual expenditure was in the millions of dollars[6].

- "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.

---

in connection with maintaining accounts and purchasing advertisements on social media sites", page 16, para 41, *ibid*.

[5] "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*.

[6] "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*.

- The Mueller indictment describes how Virtual Private Networks (VPNs) and computer infrastructure in the US[7] 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

The fact that bulk impersonation attacks have not been detected in Maryland in the past does not mean they did not happen or that they will not happen in the future. A determined actor could easily obtain bulk access to virtual ballots delivered online. Information on who votes regularly and who does not is also easily available and can be used to focus attention on those who do not vote often and hence would not know an online ballot was obtained on their behalf. 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. So there is no way of determining whether a received, voted absentee ballot was indeed cast by the voter.

Potential Impact

In the worst case, such fraud would change the outcome of the election but would not be detected. On the other hand, if fraud is suspected on Election Day, because many voters show up to vote but have absentee ballots cast in their names, it will take a while to determine that fraud did occur, and 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 will be hard pressed to explain why they ignored several letters from computer scientists urging them to address the core problem.

The use of online ballots poses many other problems as well: online ballot marking reveals the vote to any malware on the voter's computer; mailed ballots have to be reproduced by hand on ballot stock requiring a large number of expended person hours and uncertainty regarding whether the vote was reproduced correctly; the return rate of ballots delivered online is smaller than that for ballots delivered by the postal system.

[7] "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*.