AGENDA: JUSTICE AND CIVIC PARTICIPATION – MICHELE NEITZ AND KAI STINCHCOMBE

Summary of recommendations

(1) Goals-based evaluation of voting technologies

We should not allow voting technologies to drive the goals we set for voting systems, or set different standards for different technologies. For example, if we do not permit voters by and large to purposely waive the anonymity of their vote – for example, in a vote-by-mail system – then we should not allow an internet-based or blockchain-based system that would produce the same result. If we do allow this in a vote-by-mail context, we should similarly allow it in an internet or blockchain voting system. What we should not do is set a goal of moving to a new system – internet, blockchain – and reduce our security or auditability standards in order to accommodate the move.

(2) Do not adopt large-scale internet voting

Security experts generally agree that internet-based implementations of voting systems, blockchain or not, have not surmounted the inherent challenges in implementing a voting system, particularly security challenges.

(3) If adopting internet voting, do not prefer either blockchain or non-blockchain systems

In considering pilot projects, we do not find that blockchain systems are inherently better at achieving the goals – authentication and authorization, auditability, anonymity, failure reduction, and increased participation – of an internet-enabled election system. In their applications to date, blockchain-based systems rely on factors other than blockchain, such as centralized voter databases, facial ID or postal delivery, cryptographic mixing, dual-device vote validation, etc., to solve these problems. Those experimenting with new voting technologies in California are encouraged to evaluate the quality of these solutions as a whole, rather than relying on a specific technology.

(4) A call for pilots of internet voting

We encourage small-scale or low-stakes pilots, especially those designed to enable more people to vote, to provide transparency around the pros and cons of internet voting, to advance the state of voting technology, and to leverage the unique resources of California's universities, nonprofits, and technology companies.

Background: the main challenges in setting up a voting system

Authentication and authorization

The first problem of setting up a voting system will be familiar to technologists: authentication (determining that you are who you say you are) and authorization (determining that you are eligible to do what you are trying to do. When you're trying to load a Google doc or view a Facebook photo, you first log in with your username and password, and then second it checks whether you have permissions to view the content.

In the case of voting, the government creates an authorization list through the registration system, establishing who is eligible to vote. At the time of voting, the government authenticates individuals through signing names in person at polling places. Traditionally governments have used some combination of the honor system and the threat of criminal sanctions to deter ineligible registration or voting in someone else's name. At an individual scale it's not worth risking jail to vote twice, and at the scale at which it could tip elections it's very easy to detect. (The classic example is the "graveyard precincts" credited at times for Kennedy's victory in Illinois, Johnson in Texas, or Polk in New York.[0] Large-scale voter fraud like this is virtually impossible in the modern era with a well-designed voting system, but it's very much worth preventing.)

More stringent authorization and authentication is also available. Reviewing and purging the voter rolls reduces the risk of unauthorized voting, and requiring a photo ID at the polls reduces the risk of unauthenticated voting. Classically, accessibility and security are at odds,[1] and increases in security often seem designed to reduce participation rather than offer a bona fide attempt to reduce fraud,[2] which most experts believe is miniscule.[3]

Voter verifiability and auditability

Voter verifiability is the concept that the voters should not have to trust an external system certifying their cast ballot matches their intended vote.[4] The classic electronic example of this is an empty and sealed box in public view, or an ATM style machine that records the vote electronically but also prints a receipt with the names you chose and a barcode encoding those names, and then drops it in the ballot box.

The voter can see that the receipt matches their vote. The electronic totals can be spot checked against a hand count using a barcode reader – automatically in a few precincts as a spot check, or in every precinct in the case of a full manual recount, with the ballot boxes unsealed in front of volunteers, journalists, and representatives of both campaigns. And if the barcodes don't match the printed candidate names, that's easy to check. In summary, the machine-recorded all-electronic totals are instantly available, but there's also a human process – voter sees receipt, receipt is in a sealed ballot box, auditors can check the receipts after – that verifies that the electronic totals are correct.

The goal of a system that has this characteristic is that one is not left wondering if technology – either through plain error or malicious manipulation – changed the results of the voting, as many have been concerned about in the past with all-electronic systems.[5] (An all-paper system, for example with punch cards or optically-scanned marked paper ballots, obviously replicates the strengths of this system. Punch cards are vulnerable to the "hanging chads" problem, while optical ballots have a high "spoilage" rate, but there are pros and cons to every system. There are also proposals for making all-electronic systems have similar properties, such as open-source software doing cryptographic "mixing" of ballots, or independently-manufactured ballot-marking and ballot-verification machines sitting next to each other in the precinct.[5.5])

Strong anonymity

America has historically associated the secret ballot (or "Australian ballot") with not just the ability to vote secretly, but an inability to *not* vote secretly (which we'll call "strong anonymity").

The purpose of strong anonymity is, for example, to prevent an employer, labor union, commanding officer, or political campaign rounding up ballots, organizers offering the homeless money for votes, or an abusive husband asking his wife to see who she voted for. Voting secretly in a ballot box, coercion is impossible; if you can prove who you voted for, you can also be asked to show who you voted for and be held accountable for that choice.

Mail-in ballots, in the name of accessibility and increased participation, violate this principle, and have in fact both resulted in increased participation and also validated reports of fraud.[6]

Distributed decision-making as a strategy to prevent large-scale fraud

A final goal of many voting systems is to increase the number of parties that must collude (or make mistakes) to have a large-scale effect on the outcome. For example, an election run nationally on a single tabulation system by a single manufacturer would be seen as inherently more vulnerable to fraud – because the manufacturer might put a thumb on the scales, the system might be hacked, or the people administering the system might be corrupt – rather than a system spread among the states and counties, using a variety of technologies and oversight systems. Elections officials across the country have been accused of fraud and incompetence – and when the number of votes exceeds the number of voters, the accusations become quite believable – but implicitly, part of the design of our system is to minimize the impact of any given official or vendor's fraud or incompetence.

In summary, there are a set of security goals inherent in any voting system and a set of well-established best practices for addressing them.[6.5] Our first recommendation as a working group is that these principles be applied equally across technologies. We do not endorse the specific set of recommendations from Verified Vote (which, for example, conflict with vote-by-mail rules in many California jurisdictions). As the vote-by-mail example illustrates, there are tradeoffs, discussed more extensively below, between security and widespread participation. But we should not allow choice of technologies to dictate our standards – "well, with internet voting [blockchain voting, etc.] you can't do it that way, but it has other advantages" – but rather should set our standards and pick the best available technologies to implement them.

Is America ready for internet voting?

Participation and the security / accessibility tradeoff

Inherent in this discussion is a security/accessibility tradeoff. Purging the rolls and requiring identification, restricting absentee ballots, and using inconvenient technology all reduce the number of ballots successfully cast. In contrast, features like same-day registration and widespread mail voting increase turnout, at the cost of greater vulnerability to fraud. It's a matter of personal priorities – aggregated through the political process – determining how important it is to prevent various types of fraud (e.g., individual voter fraud, opportunities to pressure voters, vulnerability to large-scale manipulation) versus increasing turnout.[7]

In any expansion or reduction in accessibility, there are also tradeoffs to relative participation. ID requirements are more likely to affect the very old, or people with disabilities incompatible with driving, because they may be less likely to have a driver's license. Allowing only in-person voting disadvantages people with long commutes and less-flexible work hours. Advance registration disadvantages people with transient addresses, especially students. The level of accommodation for military personnel serving abroad might depress or increase turnout.

One can imagine that a broad goal of using technology in the voting process would be to increase turnout by people who expect to be able to transact online or from mobile devices, or for whom in-person voting is particularly inconvenient – especially wage workers, students, and digitally-native younger people, perhaps. But it will naturally also increase, on a relative basis, the participation of technology-users relative to non-technology-users.

Pilots under the UOCAVA

The earliest pilots of internet voting in the US operate under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA).[7.5] Twenty six states allow some voters to return ballots by fax and/or email, five have a web portal or mobile app, and nineteen only allow mail.[8] Few security experts would argue that fax or email voting is particularly secure or anonymous, which means that internet voting strictly improves upon these technologies –potentially both more secure *and* more convenient.

UOCAVA, incidentally, has also been the source of the first pilots of blockchain-based voting, in Denver, Utah County, and West Virginia.[9] This was the source of much controversy among cyber professionals who believe there are significant unanswered questions.[9.2]

Ironically, presumably because of heightened scrutiny around early pilots, the authentication and authorization process with Voatz, the online voting system used in these jurisdictions, is likely the most restrictive in the country – including registering in advance with a driver’s license, validating a phone number and setting a PIN, and then comparing facial recognition to the driver’s license photo.[9.3] Other enthusiasts propose composing a voter ID using fingerprint or retinal scans.[9.4]

Under the Voatz system, after voting using a mobile app, the voter receives an email receipt with an ID number and a record of their votes; the election administrator receives and publicizes the ID number and a record of the votes, but not the voter’s identity, preserving anonymity but enabling each voter to verify that their vote was counted as cast.[11.1] The emailing of the candidate selections represents a breach of strong anonymity similar to that inherent in vote by mail, but replacing the email trail with an independent-verification app or similar could fulfill the same goal eventually.

Pilots abroad and in the private sector

There have been several pilots of online voting abroad.[9.8] Estonia, an early adopter of blockchain and other technologies, has paired private keys and online access with a national ID system. Its system has been widely adopted, but independent auditors believe its security features are readily bypassed.[9.9] There are similarly significant concerns with a system adopted in Australia.[9.95] However, the technologies put in place are promising – for example, a trackable, spoilable receipt for your ballot that doesn't allow you to see what was voted, or an app with a barcode scanner that allows you to verify your vote on a system separate from the computer you're using to vote. There have also been useful innovations out of non-government voting (such as for the officers of nonprofits).[9.98]

Authentication

Among current internet voting systems, Voatz relies on a third-party service (Jumio) to match a face to a driver's license or passport photo;[9.2] Agora assumes that voter identities (e.g. distribution of public and private keys) have been established by the voting authority.[14] It is a problem one can imagine might be solved with technology at the scale of ballots for hundreds of members of the military serving abroad, but in either case there are problems with its application at scale.

Distributing private keys securely to millions of citizens (by mail or on devices) is daunting. (It's straightforward to imagine a malicious link circulated on social media designed to "validate" voting information but that actually steals passwords or ID codes that might allow an actor to vote at least thousands of times.).

An internet voting system might be more secure than in-person voting (which typically does not validate *either* a password or a face) or mail voting (which validates only a postal address). However, with internet voting the problem is more serious because a single person could steal thousands of private keys or introduce malware to the system affecting thousands of votes.[9.19] In contrast, a system to vote in person a thousand times would be much more challenging and would much more obviously expose the culprits to identification and arrest.

Validating faces against photo IDs at scale also presents unique challenges: if the system fails, what recourse does the voter have to get their face verified, for example? How do we ensure that the face recognition system doesn't have racial, gender, or age bias, as has been commonly reported across such systems?[9.21]

Security is a concern in any internet voting system

Few computer scientists with expertise in elections believe that implementations of elections protocols (such as voter authentication, ballot auditability, and anonymity) are mature enough or secure enough to be deployed at scale.[10] Security breaches are ubiquitous in online systems – witness financial companies like Equifax and Heartland Payment Systems; government systems at the State Department, OPM, and defense contractors; tech companies like Yahoo and Uber, etc.[10.5] Election systems are among the hardest to secure, because of anonymity (among other things). When your credit card is breached you receive notice after the fact because a transaction shows up in online banking, but in an secret-ballot election system the ability to verify after the fact is inherently not there.

Imagine the Florida recount on an internet system – if, after the fact, someone discovered that between 5,000 and 10,000 Florida voters made the password for their internet voting account the same as their (compromised) old Yahoo account password, and that a foreign hacker had scanned for Yahoo passwords and changed those votes on election day (or redirected the ballots, or registered to vote, or voted on behalf of some of those people, or similar). Would we have held a re-vote?

Blockchain does not meaningfully increase the security of internet voting

Many of the things blockchain enthusiasts see as the largest advantages of this technology seem to line up well with the challenges in establishing a secure voting system.

One of Bitcoin's largest innovations among digital currencies was eliminating the "double spend" problem. Having a collection of digital coins that you can spend only once *sounds* like the problem of having a bunch of digital ballots that can each be voted only once.[12] Similarly, blockchain's tamper-evident recordkeeping seems likelier to survive an audit than an ATM-style machine simply spitting out "it was 500 for this candidate and 1000 for the other one." Private-key systems generally, and blockchain among them, seem like a potential way to digitally sign ballots, ensuring that voters are actually who they say they are. Finally, digital coins like Monero have proven the ability to spend currency anonymously – perhaps, similar technologies can be used to help protect the anonymity of people's votes.

So far, however, the Working Group is not convinced that blockchain offers inherent advantages in solving the key challenges of internet voting relative to an equally-thoughtful non-blockchain solution.

In terms of inherent advantages, we have considered the four challenges outlined above.

- Authentication and authorization – It does not seem that blockchain helps with this problem. Neither password nor code distribution by mail or face comparison against previously collected face data (e.g. passport or driver's license) creates an inherent advantage of blockchain over non-blockchain systems.

- Voter verification and auditability – The best implementations for a voter casting a ballot remotely (whether open- or closed- source, blockchain or not) involve some level of trust in the user's device or devices. Often you use two devices (a mobile app and a website, or two physical devices), one of which produces a barcode or key and the other one that validates that your vote accurately represents your choices. The greatest single point of failure is the app or website or device itself.[15.7] A compromised website could display a code that validates as a vote for one candidate but transmits something different, for example.[9.2] Or malicious code inserted into the app (or a fraudulent copycat app with a confusing name uploaded to the app store, or using a malicious download link distributed on social media) could be used to forge ballots at scale.[9.19]

  In an open-source or open-standards implementation, the apps might be independently produced, which reduces the odds of failure. At this point we do not believe there is a significant gap between the way that blockchain and non-blockchain systems enable voters to validate their vote or track it auditably through the system.[15]

- Anonymity – Strong anonymity is a near-impossible challenge for any voting system that is not in-person. An employer, union, advocacy group, campaign, or abusive spouse could as easily push someone to fill out a paper ballot as an electronic one.

  Internet voting (including blockchain voting) does not appear to have incremental anonymity concerns. Clever cryptography enables you to send the votes in partial chunks to separate servers that can't individually decrypt them. Once cast, reference implementations of online voting employ a "mixing" process to separate the voters' identities from their votes. Ultimately, you have to trust the anonymization servers to behave as intended, i.e. not to be running malicious software that intercepts and decrypts incoming data. (To the extent that a malicious actor de-anonymizes ballots, their goal is presumably to intimidate and influence voters. For intimidation to work, it requires you to *know* that your ballot will be decrypted; surreptitious decryption and de-anonymization seems to be of relatively little use. But you can imagine a skilled intelligence service putting this in the Kompromat file – if a foreign intelligence service happened to know that the Secretary of State didn't vote for the President, it's a great opportunity to ask for a favor.)

Depending on the implementation, the use of time stamps in blockchain may be used to record the order of votes cast. In a small enough voting pool, this could be used to establish identifying information. If we can remove this concern without introducing new ones, however, mail voting, non-blockchain internet voting, and blockchain voting seem to be at parity in their ability to protect anonymity.[15.5]

- Reduction of single point of failure – Blockchain systems (relative to other good internet systems) eliminate some single points of failure but may introduce others.

  For example, it's positive that you can (in some blockchain implementations) choose a server to send your vote to (each run perhaps by an independent nonprofit) rather than face only a single choice. On the other hand, some leading blockchain applications are not open source, and an open-source implementation might be associated with a higher level of transparency or confidence in the results. Additionally, the number of nodes and who is running them matters tremendously for this sort of application – if a majority of nodes are all being run by the software provider, for example, it reintroduces a point of failure that was supposed to be eliminated.

  Large scale compromises of websites, computers, or apps, or theft of passwords or private keys are possible in either scenario, as are attacks on the voter registration database or human aspects of the audit systems. (See, for example, the Moscow election, conducted on blockchain, in which independent parties claim races were stolen.[16] The challenge was not a failure of blockchain, but a poor – or sabotaged – implementation, in which auditing tools were delayed or canceled.)

With these questions unresolved, the working group's second recommendation is that California not adopt internet voting (including blockchain-based internet voting) at scale.

We further believe that the operational and security issues in blockchain and non-blockchain internet voting systems are comparable, and we therefore recommend that, in considering internet voting, the State of California should not prefer blockchain internet voting to non-blockchain internet voting (or vice versa). It may be that blockchain systems are the best-developed systems available, in which case they should be used; but the focus should remain on objectively evaluating the authorization and authentication, end-to-end auditability, anonymity, and failure-protection in the system's architecture, rather than relying on promises that a particular form of technology has inherent advantages in solving any of these problems.

When are pilots appropriate?

Due to the lack of large scale pilots (especially in the US, and especially not the sort of best-case scenarios a computer security expert might desire[10.6]) we have neither failures nor successes to learn from. How large indeed are the benefits of permitting online voting, from a turnout perspective? (The West Virginia process produced 144 votes out of 183 eligible voters using the mobile app in 2018,[9.5] and pilots from the late 1990s would suggest optimism is warranted.[11] In three early cases, Voatz-eligible voters saw 5%, 45%, and 100% increases in turnout.[11.1][11.2]) What are the public and expert reactions to in-practice examples? When deployed at scale, what sets of security features produce the greatest confidence from experts, and which prove to create more barriers to participation rather than break them down?

We are less concerned about internet voting pilots when the number of eligible voters is low and the election is comparatively low stakes.

For example, we believe the number of state actors or domestic hackers willing to take the risk of attempting to hack a BART-board election is lower than the number who might be interested in influencing a presidential election in a swing state. We also speculate that the turnout advantages might be greater. Commuters who live far from where they work might be least able to use the traditional ballot box.

If there were buy-in from advocates in the relevant communities, we would also be open to piloting internet voting for specific groups where the turnout advantage could be particularly high – such as members of the military serving abroad, or people with disabilities.

In time, we hope it might be a good option for presidential elections in swing states, but we are not ready to endorse it today. (We are sympathetic to the argument that low turnout is a "flaw" of current voting systems as much as security concerns are a flaw of new ideas. As much as we may be concerned that prematurely rolling out bad election technology might sway a tight election in Florida – to use a salient example of a high-stakes election – we should also consider that rolling out election technology slowly is almost certainly *today* swaying tight elections in Florida by keeping millions at home who might otherwise vote. That said, as of today we believe the potential for critical, systemwide failure is too great to rely on internet voting today for an election like this.)

However, we do encourage pilot implementations in small-scale deployments or in low-stakes elections, as an augmentation of the existing ways to vote or as a replacement for insecure methods of military voting such as email and fax. We are especially excited about pilots designed to improve participation by populations who most likely to be impeded by current voting systems – for example, people with transient addresses or people with disabilities – and where the implementation gives the public meaningful opportunities to scrutinize the process and use what we learn to improve voting systems in the future.

Questionnaire we'd like to invite industry participants to fill out

What are the most important problems to tackle in today's voting systems:
[ ] Inconvenience (and resultant low turnout)
[ ] Falsified vote tallies (eg hacked, manipulated)
[ ] Unauthorized voting (eg noncitizens, double voting, etc)

Which problems in voting do you think are the most challenging:
[ ] Keeping a list of registered voters
[ ] Authenticating voters at the time of voting
[ ] Voters knowing their vote was recorded correctly
[ ] Chain of custody, accuracy, auditability between voting and tallying
[ ] Protecting voter privacy / anonymity

Enabling people to vote using the internet (e.g. on laptops or phones) as well as by mail and in person could result in more people voting, but might also introduce new vulnerabilities. Do you think the US is ready for internet voting:
[ ] No

[ ] It would be interesting to see some small-scale pilots
[ ] Blockchain systems would work, but not without blockchain
[ ] Blockchain or not, we should do it

Part of what we are trying to do here is isolate the advantages of blockchain-based systems from the most comparable alternatives – for example, are we really talking about an advantage of blockchain as a technology or a broader advantage of free and open-source software?

Relative to a high quality, open-source internet voting system that does not incorporate blockchain, what is the problem that you think blockchain could improve most and how would it help?
[ ]
[ ]

Are there problems relative to a high-quality, open-source non-internet voting system (e.g., an ATM-style system that prints a voter-verifiable paper trail) that we should be solving using blockchain? If so, what problems and how would they help?
[ ]
[ ]

[0] Ellen Sauerbrey says dead people voted in Maryland last year; An Old Cook County Tradition
[1] Stevey's Google Platforms Rant
[2] Purges: A Growing Threat to the Right to Vote
[3] The Myth of Voter Fraud; The Truth About Voter Fraud
[4] What Is a Voter Verified Paper Audit Trail (VVPAT)?; Why paper is considered state-of-the-art voting technology
[5] Ohio's Odd Numbers; Was the 2004 Election Stolen?; How to Rig an Election
[5.5] Stop the Presses: How Paper Trails Fail to Secure e-Voting
[6] Vote Harvesting: A Recipe for Intimidation, Coercion, and Election Fraud; How Ballot-Harvesting Became The New Way To Steal An Election; Election Fraud in North Carolina Leads to New Charges for Republican Operative; see also Secret ballot - Wikipedia

[6.5] Verified Voting Foundation: Principles for New Voting Systems; see also ProCon.org's summary of positions on voting machines by the National Academy of Sciences
[7] In some cases, reducing turnout is a political or ideological goal. We assume that in California the overall preference is for systems designed to encourage turnout. Additionally, citizens whose primary goal is reducing turnout are unlikely to be enthusiastic about blockchain voting.
[7.5] https://www.fvap.gov/uploads/FVAP/Policies/uocavalaw.pdf
[8] Electronic Transmission of Ballots
[9] Under the Hood: The West Virginia Mobile Voting Pilot; Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it; Utah County, Utah, begins review of mobile-app votes; WV Secretary of State – 24 Counties to Offer Mobile Voting Option for Military Personnel Overseas
[9.2] What We Don't Know About the Voatz "Blockchain" Internet Voting System
[9.19] Going From Bad to Worse: From Internet Voting to Blockchain Voting at 6 (**"**Exploitation is often imperceptible to a user, and can often be done so undetectably that a forensic
examination of the device will not reveal malware's
presence.")

[9.21] Voatz states that in 99.2% of approximately 100,000 cases to date, voters' faces were automatically identified, and that all of the other 0.8% have succeeded with a fail-over to human verification.[11.1] We encourage government officials to take the risk of racial bias extremely seriously. However, we are sensitive to the racial bias in existing systems – long lines at certain polling places and not others, for example – and so ask ourselves the question, would the net impact of offering driver's-license-based facial recognition internet voting be a reduction or enhancement in the ability of voters from minority groups, particularly dark-skinned voters, to express themselves equally? If we cannot establish that it is an improvement, we cannot permit such a system to move forward. However, if we conclude that new technology will reduce voting barriers faced by underrepresented minorities, we cannot ignore that conclusion either.
[9.3] Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it

[to do: condense into a parenthetical aside]
Just as the dot-com bubble enabled two now-defunct internet-voting sites (Votation.com and VoteHere.net) to raise significant venture capital,[13] it's possible that the current glut of available funding for blockchain startups will represent an advance on existing technologies.[13.5] Supposing there is a spectrum of blockchain skepticism to enthusiasm, even the most skeptical skeptics might find that the best providers of

internet voting are offering blockchain-based solutions because it's easier to raise venture and hire a strong team. For example, video-based authentication such as offered by Voatz may prove to solve a meaningful problem unsolved by any other vendor of internet voting technology; the blockchain aspect may be deemed irrelevant (or even abandoned in the long run) relative to other value propositions.

[9.4] Opinion | It's Time for Online Voting
[9.5] Internet Voting Is Becoming A Reality In Some States, Despite Cyber Fears
[9.8] Online voting is impossible to secure. So why are some governments using it?. For a 2017 not-comprehensive list of companies doing online voting, see here: Nine Companies That Want To Revolutionize Voting Technology
[9.9] Security Analysis of the Estonian Internet Voting System and associated Press Release.
[9.95] The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election
[9.98] Solution Overview: Online Voting Security and Verifiability
[10] If I Can Shop and Bank Online, Why Can't I Vote Online?
[10.5] Going From Bad to Worse: From Internet Voting to Blockchain Voting at 6; The 18 biggest data breaches of the 21st century; Every single Yahoo account was hacked - 3 billion in all; Krebs on Security: Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen; The OPM hack explained: Bad security practices meet China's Captain America; New details emerge about 2014 Russian hack of the State Department: It was 'hand to hand combat'; Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies
[10.6] Ironically, if we imagine that IT professionals are divided among skeptics and enthusiasts, we might be more interested in pilots designed by the skeptics than the enthusiasts.
[11] See Electoral Insight - Technology in the electoral process for some examples from the late 1990s.
[11.1] Nimit Sawhney, interview with Working Group..
[11.2] Note also the admittedly-small-n study of the West Virginia pilot: "I estimate that the ability to vote with a mobile device increased turnout by 3-5 percentage points, a large effect relative to other electoral reforms… [the analysis] suggests that 46 individuals voted who would have not otherwise voted if mobile voting wasn't an option. In the counties being studied (excluding Harrison and Monongalia), 107 individuals actually cast a ballot using the mobile app. This suggests that just over half the people using the mobile app would have voted anyway had the app not been available, but almost half the people using the app were induced to vote because of mobile voting." Promises and Perils of Mobile Voting
[12] Opinion | It's Time for Online Voting

[13] Internet voting: A touchy issue; VoteHere's technology ends up in the hands of Election Trust
[13.5] Are Blockchains the Answer for Secure Elections? Probably Not
[14] Agora: Bringing our voting systems into the 21st century (Whitepaper Version 0.2)
[15] See e.g. Election Trust and compare to Agora: Bringing our voting systems into the 21st century (Whitepaper Version 0.2)
[15.7] According to https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/ and https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/
99% of US-based mobile phones are running operating systems created by California-based companies Google and Apple. These systems typically include security features – code-signing, HTTPS enforcement, biometric verification, protections against certain activities of malware – that are not common on all internet platforms. We are excited about the opportunity to leverage the security features to help increase the security of internet voting relative to what might have been possible a decade ago.
[16] Shut up and trust them Why Moscow's new Internet voting system relies on faith, not transparency or peer review; Libertarian Party of Russia (via Telegram)