Merle King Quotes

Concerns over election hacking misplaced but not unfounded
By CHARLES TAYLOR Oct. 2, 2016

http://www.naco.org/articles/concerns-over-election-hacking-misplaced-not-unfounded
There are more than 9,000 election jurisdictions in the United States, according to Merle King, executive director of the Center for Election Systems at Kennesaw State University in Georgia. He said that while registration databases have been accessed by hackers, the possibility of voting machines' being compromised is "highly improbable" because, by and large, they are never connected to the internet. "They have multiple internal and external verification procedures to ensure that all of the votes that are cast by the voters and tabulated by the systems are validated," he said.

https://www.seeker.com/vote-recount-how-it-can-help-future-elections-2117767875.html

An opposing view is held by experts like Merle King, executive director of the Center for Election Systems in Kennesaw, Ga. King says that every voting machine has a small error rate. If the outcome of the election falls within the error rate, the number of votes will change each time the ballots are recounted.

"The question is whether the recount will illuminate other issues such as bad ballot design, the lack of accessibility or deficiencies in the voting technology," said King, who consults with state and local officials in several states. "The answer is no."

King suggests that the numbers for Clinton and Trump will probably change. That's because the optical scanners that record the ballot marks "see" things differently each time they are used.

"What you are going to see in this recount is the numbers will change," King said. "It's a change in the sensitivity of scanners."

If the numbers come back exactly the same, then some people will think that something is wrong, King said. But if they come back different, others will say that the count is wrong as well.

"Either way you will get differences in the totals produced," he said.

….

"This election has illuminated the vulnerability of election systems to real and perceived hacks," King said. "There is a high level of anxiety in citizenry about conduct of elections. That's an emotional response. It's hard to address an emotional response with a technology."

http://www.mydaytondailynews.com/news/national-govt--politics/hacking-the-ballot-how-safe-your-vote-this-november/ZrAhN7lRsXve1rTgmUnAkJ/No ‘DEFCON 3’

Elections system researcher Merle King said he is confident in the country’s voting systems.

“I have not gone to DEFCON 3 yet,” said King, executive director of the Center for Election Systems at Kennesaw State University in Georgia. “I don’t think we are going to see attacks and hacks that alter the outcome of the election that are undetectable.”

But King and others said there are vulnerabilities in other parts of the the nation’s election systems, specifically voter registration, online ballot delivery and Election Night vote reporting, which does use the internet. Of particular concern is that online voter registration rolls could be vulnerable to hackers and experts say more needs to be done to make sure that the information in those databases is not compromised or used for fraudulent purposes on Election Day.

http://mashable.com/2016/09/26/election-voting-system-analysis/

A centrally-managed voting system sounds like a prime target for hackers, but Georgia's Center for Election Systems Executive Director Merle King explained that the system is actually an almost even split of centralized and decentralized. So the management of the ballot creation, voter rolls and system tests are all centrally managed at the university. However, the state election lists or electronic books are then burned to media on dedicated machines and hand-delivered to each county, so no portion of the voter rolls goes over the Internet or a network.

…

Considering that most experts I spoke to seemed uncomfortable with the continued use of direct-entry electronic voting systems, I had to wonder why Georgia was one of the rare states still using them.

“That’s a loaded question: Are we stuck with it or are we visionary?” chuckled King, who contends that most election fraud is conducted via paper ballots, and mostly through absentee ones.

“When jurisdictions adopt paper, many of the reasons are good reasons, but it’s not to make election more secure,” contends King.

“The idea that you’re using last year’s iPhone or iPad and you’re out of date does not apply to voting tech. You’re still just counting by one. That’s all [these voting systems] do. The notion that age is the equivalent of obsolesce is a fallacy,” he said

…

https://www.buzzfeed.com/sheerafrenkel/these-5-points-show-just-how-hard-it-is-to-hack-an-election?utm_term=.epvawq5wP

Once the voting is over, local polling officials take the results from each individual machine and transfer it onto a server. (Neither the machines nor the servers are online or have ever been connected to the internet). They then copy the information onto a USB stick (again, one that has never been used and “flashed” to make sure it is empty).

The unofficial results are tabulated that night and sent electronically to the each state’s office of the secretary of state, said Merle King, executive director at the Center for Election Systems at Kennesaw State University. He added that local officials perform a “reasonableness check” to make sure that the results coming in make sense. Even if the results are somehow electronically intercepted mid-way, the local officials still have the original data stored and can re-send results.

“No voting system has an internet interface. None of these systems are online,” said King, emphasizing why the original results would not change. “There is a lot of attention paid to that, to none of the servers being online. “

It takes 5–6 days until after the elections for the official results to be tallied. Local officials burn one copy onto a CD that they keep in their office, and another is burned onto a CD that is hand-delivered, usually by local police, to the offices of each local secretary of state.

If someone wanted to interfere with the results, they would need to be physically present and tamper with the CDs or USB sticks. King said there are multiple local officials in the room, including local representatives of the Republican and Democratic parties, police, and volunteers.

Time http://time.com/4500216/election-voting-machines-hackers-security/

“Merle King, the executive director for the Center for Elections Systems at Kennesaw State University and one off the preeminent election experts in the country, added that the prospect of the election being hacked by cyber ne'er-do-wells is "totally improbable." "It just can't really happen," he said.
….
“King, the election expert at Kennesaw State University, put it more bluntly. "It's very far-fetched, actually," he said. The more more worrisome threat, he added, is that these criminals affect Americans' perception of the integrity of the election results. "If there was something that came up, even on a small scale, that compromised people’s perception of the legitimacy of this election," he said, "that would be the worst outcome—that could be really terrible.”

http://www.mcclatchydc.com/news/politics-government/election/article99602862.html

“Adding layers of communication and coordination and perhaps decision-making may not only not help, it may actually hurt the integrity of the election by slowing it down,” explained Merle King,

executive director of the Center for Election Systems at Kennesaw State University in Georgia, which provides technical support to the state.

It is also important to note that because election officials have come to expect certain problems, they are trained to catch mistakes throughout election day: "Elections are essentially a human event. You have tens of thousands of humans with some degree of training that come together for this event, and they make mistakes," said Merle King, who worked at The Center for Elections Systems at Kennesaw State University.

http://www.businessinsider.com/experts-explain-why-the-election-would-be-almost-impossible-to-rig-2016-10

“While no election will ever run without glitches and hiccups along the way, for an election to be successfully hacked with malicious intent, a person not only needs to know how to alter the code of the machines, but also know how to alter it in a way that would not be easily discovered and flagged in post-election audits.

"In this election one of the biggest concerns is the undermining of confidence in the outcome of the election," said Merle King. "And in every election, there's going to a loser of that election." “

https://thevotingnews.com/tag/merle-king/

Georgia: Elections officials: Floyd County Faulty voting machine contains 85 votes | RN-T.com
Aug 2 2012
» The Voting News

Floyd County Elections Board Chairman Pete McDonald said the malfunctioning touch screen voting machine at Alto Park has been sent to the manufacturer in an attempt to access the 85 uncounted votes it holds. McDonald said Merle King at the Georgia Elections Center at Kennesaw State University reported that attempts to retrieve the election data from the memory card or from the archive memory were unsuccessful.

“We tried unsuccessfully Tuesday evening to process the votes on the machine and the Georgia Elections Center staff have also been unable to process the votes from the machine,” McDonald wrote in a press release Wednesday evening. “The voting machine is being sent to the ES&S (provider of the Georgia elections system) center in Omaha for a resolution.” The balance of the votes from the Alto Park precinct will be processed and added to the total vote count by Friday, he said.

http://www.thedailybeast.com/all-50-states-ask-feds-to-help-them-stop-election-day-hackers
“States have been preparing for this election for two years. The gear is ready. The election workers have been trained,” Merle King, the executive director of the Center for Election Systems at Kennesaw State University, told The Daily Beast. “Although many of the issues surrounding election and voting systems that have made headlines in the past year are new to the public, they are not new to election officials.”

…

Poll books “have been scanned, hardened, and are under continuous monitoring throughout Election Day and Election Night,” King said. “These systems have redundant components and can be quickly recovered if an anomaly occurs.”
…

“The residual vote rate has evolved into a metric of the accuracy and effectiveness of a voting system,” said King. “In this election, there is expected to be a larger-than-usual number of voters who skip the top two races… This could lead to a false positive regarding the accuracy and security of the voting system.”

https://www.washingtonpost.com/news/monkey-cage/wp/2016/11/07/a-cyberattack-could-disrupt-tuesdays-u-s-elections-but-wouldnt-change-the-results/
A cyberattack could disrupt Tuesday’s U.S. elections — but wouldn’t change the results
By Charles Stewart III and Merle King November 7, 2016

http://www.daytondailynews.com/news/national-govt--politics/what-six-experts-say-about-election-rigging/uma3tboRxBB9mH9zLuSBKK/

Merle King, executive director, Center for Election Systems, Kennesaw State University, Georgia: “In order to sweep an entire state in a hack, the conspiracy would have to be so large that if all the conspirators simply went to the polls and voted they would carry the election.”

http://www.dw.com/en/why-hacking-the-us-elections-is-extremely-difficult/a-36035723

While breaking into election technology that is connected to the internet - like voter registration systems - is less difficult and has been done before, those systems have been hardened in response to the DNC hack, said Merle King, executive director of the Center for Election Systems at Kennesaw State University. What's more, the rationale for hacking into databases like voter registration systems is usually not political, but criminal, namely to get access to a large batch of personal information, he noted.

That's not to say that compromising the election systems should not be a concern or is impossible, rather that the systems currently in place are up to the task - even if some of them are old.

"The challenges for people that read stories about the ageing voting system is to understand that age doesn't equal obsolescence and that the functionality of the voting systems doesn't change over time," said King. "We still fly B52 bombers in our Air Force because they still get the mission done and they are economical to operate."

http://www.dos.pa.gov/VotingElections/Documents/Election Policy Summit Presentations/Wendy Underhill Presentation.pdf

Words from the wise
“Choose a system that can respond to not only the demands of today, but the desires of ten years from now.” --Merle King, Executive Director, Center for Election Systems, Georgia

Merle King On Election “Hacking” Fears

By Doug Chapin September 1, 2016

http://editions.lib.umn.edu/electionacademy/2016/09/01/merle-king-on-election-hacking-fears/

“When I hear about a hack, and it’s attributed to a Russian IP address, my first reaction is it’s identity theft,” King said. “They’re looking for large lists of critical information that can be used to create identities for credit card theft, etc. I don’t instinctively think it’s an attack on our election system.”

The important point King makes is that hacking the elections system and the voting system are very different in nature and effect. “If the election systems were hacked, there are paper backups of the electors list — every precinct has to maintain a paper copy of the voter list — so you could disrupt an election by attacking those election systems,” he said. “But most importantly, you could not alter the outcome of the election by hacking those systems. That would have to occur in the voting system” — the actual process of casting ballots. And that’s harder than it seems.

…

There are caveats, of course. For one thing, a hack of the voter registration database could make it easier to identify voters who could be used as targets of fraud (people who are dead or who don’t vote often). There can be tampering by campaign officials. And no system, no matter how well-protected, is unhackable, including the listed process above.

Each of those caveats is very unlikely for a number of reasons. Voter fraud is far, far harder than it seems, requiring a lot of people to break federal law for it to approach any sort of meaningful scale. Sure, some elections are won by a few hundred votes — but tipping that election means finding a few hundred people to cast ballots in the right place ahead of time. That’s harder than it may sound. Campaign officials can and have toyed with results, but being caught means losing a job and prison time — with the problem of scale still looming. The process above could conceivably be hacked, I guess, but if you can figure out how to do it without being caught, you could probably get a lucrative job somewhere else much more easily.

Merle also puts his finger on a key challenge for election officials: how to respond to allegations which can’t be disproved:

“As an election official, I frequently find myself challenged to prove the negative,” he said. “The conspiracists never have to prove their theories, but the election official has to prove the negative, which we know is impossible to prove. Can I prove that the Arizona system was not hacked by Russian state operatives? I cannot.”

https://www.bloomberg.com/features/2016-voting-technology/
“This is the strangest niche of IT that I’ve ever come across,” says Merle King, executive director for the Center for Election Systems at Georgia’s Kennesaw State University, which runs the state’s vote machine testing program. “Whatever you think you know about IT, you have to check it at the door. It’s legacy stuff, but it’s legacy in weird ways. This is legacy stuff that as you start to tease it apart goes back decades.”