STATE OF WISCONSIN CIRCUIT COURT

DANE COUNTY BRANCH 3

In the Matter of the Recount of Votes for President of the United States:

JILL STEIN vs. WISCONSIN ELECTIONS COMMISSION

Case No. 16CV3060

HEARING November 29, 2016
The Honorable Valerie Bailey-Rihn, Presiding

NOTE: This transcript has been edited to shorten and reorganize some exchanges for clarity and brevity. Most of the courtroom procedure (e.g., asking for further questions, overruled objections) has been omitted, as have most of the niceties (e.g., "Yes, I understand. Thank you"). Some commentary has been added. The full official transcript is at http://bit.ly/2wZA3IO .

Before the Wisconsin Presidential recount in 2016, the Jill Stein team sought a court order requiring votes to be hand-counted, not just run back through the voting machines. As you will see, Judge Bailey-Rihn decided to allow counties to use voting machines in the recount. She explained that Wisconsin law gave her little choice, allowing county boards of canvass the leeway to choose either machine or hand counts unless the plaintiffs could provide hard evidence that the machines would miscount the recount, and that a true count would result in a different outcome.

The Judge acknowledged the Catch-22 nature of a statute that requires evidence of electronic miscounts before a hand count can be ordered, though that evidence cannot be collected without a hand count. At the same time, she made it clear that the testimony had established that hand counts were the only reliable way to verify accuracy.

Nevertheless, the arguments and expert testimony captured in this transcript will be valuable for any future efforts, in any state, to promote hand-counting as a means to verify computer-tabulated election results.

Attorneys for the Stein Campaign:

Matthew D. Brinckerhoff, Debbie Greenberger, and David Lebowitz; Emery Celli Brinckerhoff & Abady, New York, New York
Christopher M. Meuler; Freibert Finerty & St. John, Milwaukee, Wisconsin.

Testimony for the Stein Campaign:

J. Alex Halderman, University of Michigan Computer Science
Philip B. Stark, University of California-Berkeley Statistics
Ronald Rivest, Massachusetts Institute of Technology, Computer Science

Attorneys for the Wisconsin Elections Commission:

Assistant Attorneys General S. Michael Murphy, Colin Roth, David V. Meany, Andrew Cook, and Anthony Russamanno, Wisconsin Department of Justice

Testimony for the Wisconsin Elections Commission:

Michael Haas, Wisconsin Election Commission, Madison, Wisconsin

Others:

Attorneys Joshua L. Kaul and Charles G. Curtis, Jr., appearing on behalf of Secretary Hillary Clinton.

Testimony of J. Alex Halderman, for the Stein campaign

J. Alex Halderman, U Michigan Computer Science

Direct Examination

HALDERMAN: My full name is John Alexander Halderman, although I usually go by J. Alex Halderman.

I'm a professor of computer science and engineering at the University of Michigan and the director of Michigan Center for Computer Security and Society. I am an expert in computer security, network security, and the security of electronic voting systems.

I have extensively studied the kinds of electronic voting machines and voting systems that are used in the United States and other countries including ways in which they might be compromised by attackers as well as methods for improving their security.

I've been involved in government-sponsored studies, including the California Top-to-Bottom Review, which examined optical scan voting machine security.

Stein Attorney Matthew Brinckerhoff

STEIN ATTORNEY: And are there any kinds of security problems just in general that you're aware of or have identified or become familiar with in the years that you've been working in this area?

HALDERMAN: Yes. Optical scan voting machines are computers. Just like other computers, they are subject to security problems. Somebody who attempted to hack into an optical scan voting machine could cause it to count votes incorrectly and produce any outcome that they wanted.

STEIN ATTORNEY: Have you had an opportunity to review any of the affidavits or materials that were submitted by the Wisconsin Elections Commission earlier today?

HALDERMAN: Yes, very briefly.

STEIN ATTORNEY: Based on that brief review, do you have any opinion about whether or not the safeguards that are in place in Wisconsin to prevent some kind of outside cyber interference with optical scanning machines specifically gives you any degree of comfort that they are secure?

HALDERMAN: My understanding is that those safeguards include pre-election testing, and they include tamper evidence seals. Those are not effective at preventing cyber-attack against voting systems. We know from extensive research that seals and pre-election testing can be completely bypassed by attacks on the machines.

STEIN ATTORNEY: Let's start with the seal. Can you describe for me what the sealing security measure is and why it can be bypassed in the way that you just described?

HALDERMAN: A tamper-evident seal is supposed to show that a voting machine has not been physically tampered with. Unfortunately, security experts have demonstrated that the kinds of tamper-evident seals typically used on voting machines are easy to bypass by an attacker with simple and readily available tools. And by bypassing them, you can tamper with the voting machine without leaving evidence that's going to be detected when the seals are checked as part of normal election procedures.

STEIN ATTORNEY: And insofar as you can, what kind of available tools are you referring to when you speak of the tools that could be used to bypass the seal?

HALDERMAN: Well, depending on the kind of seal, it might be something as simple as a screwdriver or a hair dryer that can be used to loosen the seal or remove it in a particular way without leaving evidence of tampering.

STEIN ATTORNEY: And if there is no attempt to compromise the integrity of the voting machines by physical means in the way that you described, are there other methods available to someone to try to change the potential outcome of the vote tally?

HALDERMAN: Yes. Unfortunately, physical access is not required to tamper with optical scan machines and other kinds of voting machines. Even though they may not be connected to the Internet directly, these machines receive software updates, they receive ballot programming from other equipment either at the offices of a county government or perhaps at a company that provides services to the county.

Those other systems may be connected to the Internet or may be attacked in other ways. And once the systems that are used to program the voting machines are compromised by an attacker, the attack can spread on the removable media that's used to configure the voting machines into the machines themselves, and that requires no compromise of any seals.

STEIN ATTORNEY: And are you familiar with whether or not the State of Wisconsin and specifically the Wisconsin Election Commission has any private company vendors that do any of the operating of the voting equipment on Election Day?

HALDERMAN: Based on material that I've reviewed, there are examples of companies that service a thousand or more different polling locations in Wisconsin. The worry would be in my mind that that company if compromised could be used to spread an attack to all of the poll sites that it services.

STEIN ATTORNEY: Now, one of the other things in addition to the seal that you mentioned is that there's a certain amount of testing that is done of optical scan machines leading up to their use on Election Day, correct? What kinds of problems arise, if any, in the effectiveness of that particular technique?

HALDERMAN: The pre-election testing requirements in Wisconsin and other states are designed to demonstrate the logic and accuracy of the machine is functioning correctly. That is, that the ballot has been set up properly and mechanical factors like that. It's not designed and does not function to detect cyber-attack against the machines.

The logic and accuracy test can be defeated by malicious attacks in a number of different ways, including by having the attack only function if the machine has counted a large number of votes, larger than the number that are tested in pre-election testing, or perhaps by setting the time at which the attack will function to be towards the close of polls rather than prior to the opening of polls when the logic and accuracy tests are performed.

STEIN ATTORNEY: Have you yourself ever attempted to hack into a voting opscan machine to attempt to alter the way it would operate?

HALDERMAN: I myself have been involved in studies that have demonstrated the vulnerability of opscan machines, including the California Top-to-Bottom Review. I have in my own work constructed attacks against DRE voting machines that would function similarly to the way an attack on opscan machines would function, by spreading in the form of a voting machine virus from one point of infection to many machines.

STEIN ATTORNEY: And is there a difference between a virus and what sometimes is referred to as malware?

HALDERMAN: A virus is one form of malware. In this case, a virus is a form of malware that can spread to machines sometimes not connected to the Internet by ‘hitching a ride’ on the memory cards that are used to program the voting machines on Election Day.

STEIN ATTORNEY: Just so I understand specifically what you mean, when you say "hitching a ride," what is happening physically if there's malware or a virus that's infected a computer system at a manufacturer or at the primary computer base for an election system within a state. How does it exactly hitch its ride to these individual machines?

HALDERMAN: The specifics would depend on the particular voting system involved, but in general, the malware would modify or add files to the memory card that would cause the voting machine to malfunction in a way that it miscounted votes. For certain kinds of voting machines we know that the malware on the memory card can modify the programming inside the voting machines in a persistent and potentially undetectable way.

STEIN ATTORNEY: I think you are familiar with the fact that one of the issues presented today in this case is whether there's an important distinction between recounting ballots by hand versus running the same ballots through the machines after they've been reprogrammed. Is there any way in your expert opinion that that a person bent on infecting that machine could accomplish that both in the election and in the recount?

HALDERMAN: Yes. The same vulnerabilities that were present on Election Day continue to exist in the voting machines because they are the same technology, the same model. For that reason the machines are just as subject to hacking now as they would have been prior to the election.

STEIN ATTORNEY: And is there any possibility that if someone had initially gotten malware or a virus to hitch a ride into one or more opscan machines, that it could remain there in some way and affect further operation even if it is subject to some kind of reprogramming with new memory cards and the like?

HALDERMAN: Yes. Because some of the programming in a computer is persistent programming. It doesn't exist on the memory card. It's in the firmware inside the device. And as I have shown in my research on certain models of voting machines, we can persistently reprogram that firmware to cause the machine to continue to be dishonest to cause fraudulent results in future elections or recounts.

STEIN ATTORNEY: And do you have an opinion based on your testimony thus far of what kind of a recount would be most reliable, a hand recount where the ballots are examined by human eyes and hand tabulated, or a rescan through the same machines with a new program?

HALDERMAN: I am of the strong opinion that a hand recount is going to provide a more accurate result because it will not be affected by any kind of cybersecurity attack that might be compromising the scanning machines.

STEIN ATTORNEY: Are you familiar with the types of optical scanning machines that are used in Wisconsin?

HALDERMAN: Yes, I am.

STEIN ATTORNEY: Are you confident that a rerun through the machines will be accurate?

HALDERMAN: I am not confident that a rerun through the machines will be accurate. Optical scan machines have been demonstrated in research to suffer from a wide variety of not only security problems but also problems with their accuracy.

STEIN ATTORNEY: Is there anything about this particular election cycle that leads you to have any specific concerns about cybersecurity when it comes to the integrity of the election systems within the United States at large?

HALDERMAN: Yes. I'm concerned because in this election cycle we've seen unprecedented cyber-attacks, reported by the federal authorities, that appear to have been aimed at interfering with the course of the election.

These include attacks on the e-mail system of the Democratic National Committee, the e-mail of John Podesta, the Hillary Clinton campaign manager, and include attacks aimed at the voter registration systems of two states, Illinois and Arizona, as well as attacks that reportedly were attempts to infiltrate election systems in I believe it was twenty other states that have been reported.

STEIN ATTORNEY: And at least within the United States, have there been other attacks that you're aware of or attempted attacks specifically targeted at election-related activities, whether it's a campaign or election official websites and the sorts of attacks that you just described?

HALDERMAN: These are, to my knowledge, a pattern of attacks and especially one linked to foreign government that does not have precedent in an American Presidential election.

STEIN ATTORNEY: And do you have any familiarity of any attempted or successful types of cyber-attacks into elections in other countries in the world?

HALDERMAN: In the 2014 election in Ukraine, there was, according to published reports, an attack that targeted the election infrastructure

STEIN ATTORNEY: Based on the nature of the attacks that you described within the United States, do you have any opinion about the sophistication or abilities of the person or persons who carried out one or more of those attacks?

HALDERMAN: My opinion is that the pattern of attacks that we've seen follows the mode of operations commonly associated with nation-state style attackers, foreign states, and their cyber military capabilities. These capabilities are among the most powerful threats known to computer security.

STEIN ATTORNEY: And why is it that they are in that rarified category that you just described?

HALDERMAN: Nation-states in their cyber offensive capabilities often target very well-hardened and secured systems and yet have methods of breaching them, such as what we call ‘jumping an air gap’ which means targeting a computer or other device isn't directly networked to Internet connected devices or other systems that might be attacked. Instead, there's some kind of physical disconnection between the systems.

STEIN ATTORNEY: And I'm sorry to jump a little bit around, but let’s go back to the hand tabulating or hand counting of the vote. Do you have any opinion about any risk of human error in that kind of compilation? Human error in the hand tabulation of the vote?

HALDERMAN: Yes. My opinion is that the risk of human error in hand tabulation is low. In hand tabulation of a single race, the procedures in Wisconsin call for ballots to be sorted by the chosen candidate and then the number of ballots for each candidate to be counted. These are simple and straightforward steps. *(Note: The votes are also counted at least twice, by different people. This redundancy acts as sort of an ongoing verification of the totals. Electronic counts have no similar redundancy.)*

STEIN ATTORNEY: And is there any opportunity in a hand recount for someone to electronically through malware or any of these kinds of activities influence the outcome or the tallies of the vote?

HALDERMAN: No. And that is the very point of having a paper record. The paper record provides a very strong defense against attempts to manipulate the election outcome through cyber-attack because the paper itself obviously is a physical record, cannot be changed by cyber-attack after the votes have been cast. And thus, the paper record ends up being the most reliable indicator of the intent of all of the voters.

STEIN ATTORNEY: And is there anything about the State of Wisconsin in this election cycle that you believe makes it more vulnerable or likely to be targeted by potential cyber-attackers of the sort that were confirmed leading up to the election?

HALDERMAN: Wisconsin was among the states that were predicted to have very close races in the Presidential election. An attacker planning to commit an attack that would disrupt or change the outcome of the Presidential election would logically want to target the close states because those are the place where an attack would likely have the most probability of affecting the overall outcome.

STEIN ATTORNEY: But isn't it also true that as long as you change enough votes, you could change the outcome of a vote in a state that was not prognosticated to be as close as Wisconsin?

HALDERMAN: That's true, but the more votes you change, the more likely the attack would be to cause people to be suspicious. So thinking in the role of an attacker, the best strategy is to attack the states that are predicted to be the closest.

Cross-examination

STATE ATTORNEY: You've not identified any specific attack on a Wisconsin vote tabulation machine, or any instance of a Wisconsin vote tabulation machine being compromised, right?

Ass't Atty. General Michael Murphy

HALDERMAN: I have not, though the evidence of that would come from the paper record and by comparing that to the digital record. *(Note: At least two instances of voting machines compromised by misprogramming are known. Had this question been asked, under oath, of WEC Director Haas, he would told of the Stoughton and Medford miscounts—both electronic miscounts by opscans, both confirmed by hand counts.)*

STATE ATTORNEY: And you're not aware of any malware currently on a Wisconsin election tabulation machine?

HALDERMAN: I don't know of any malware presently on the machines, but the evidence of the malware would come from inspecting the paper ballots.

STATE ATTORNEY: And you don't know what kind of seals are used in Wisconsin on the machines?

HALDERMAN: I know the types of seals that are typically used in election systems in the United States.

STATE ATTORNEY: And you've not physically reviewed or investigated any of Wisconsin's machines or the security procedures used in this election; is that right?

HALDERMAN: Yes, I have investigated and tested some of the models of electronic voting machines used in Wisconsin. I haven't conducted the investigations within the borders of Wisconsin.

STATE ATTORNEY: So you haven't conducted any that have been tested by the Wisconsin Election Commission? The question is not models; the question is machines.

HALDERMAN: The individual machines, no, I have not. *(Note: Neither has the WEC. They test only models provided by the voting-machine companies at the time of state certification, not the actual machines provided to the municipalities, to be used in polling places.)*

STATE ATTORNEY: And you're not aware of any malware on election tabulation machines in Wisconsin that would affect a recount in the way that you described would be possible.

HALDERMAN: I'm not aware of such malware, although, such malware could certainly be constructed.

STATE ATTORNEY: So would a comparison between the ballots that were fed through a machine and the output of the machine based on those ballots tell you whether the counting had integrity?

HALDERMAN: No, necessarily. It depends on, for instance, the size of the count.

STATE ATTORNEY: Okay. So comparing the output from the actual ballots would not let you know if the machine was counting correctly. Is that your testimony?

HALDERMAN: Counting the ballots by hand and comparing them at scale to the output of the machines on Election Day would tell you whether the machines had been counting correctly.

STATE ATTORNEY: Is it true that you have written articles about the integrity of the 2016 general election, and publicly stated that deviations between the election results and the polls were probably not the result of a cyber-attack? That the more likely explanation is that the polls were systematically wrong?

HALDERMAN: Yes, although I don't think the cyber-attack is orders of magnitude less likely than the deviation from the polls.

STATE ATTORNEY: It's fair to say that your testimony here about the dangers and hazards are about possible problems with Wisconsin voting machines, and not what has actually happened as far as you're aware, right?

HALDERMAN: Vulnerabilities of this magnitude are an actual problem with the Wisconsin voting machines. *(Note: Nice answer. We have to keep pounding that in: the risk of undetected miscounts is a problem. When your car's brake warning light comes on, you have a problem. You don't have to wait until you crash.)*

STATE ATTORNEY: But we went through a number of questions where you don't have any evidence of any of those problems occurring in Wisconsin, right?

HALDERMAN: If the problems occurred in Wisconsin, it is possible that the only evidence would be on the paper ballots and will only be detected if a hand count is performed.

Redirect examination

STEIN ATTORNEY: Have you been provided any opportunity to inspect any of the machines that were used by Wisconsin in the 2016 Presidential election?

HALDERMAN: No, I have not.

STEIN ATTORNEY: Would you be willing to conduct such an inspection?

HALDERMAN: Yes, I would.

STEIN ATTORNEY: And if you inspected any, would you be able to conclude definitively whether or not there was some kind of cyber-attack that affected the outcome of the election here in Wisconsin?

HALDERMAN: I cannot say for sure without performing such an inspection, but such an inspection would have a significant likelihood of revealing the presence of such a cyber-attack if one had been conducted. The method to be confident that such a thing is detected is hand counting every ballot.

STEIN ATTORNEY: Now, you were questioned about the types of seals. Are there any kinds of seals, given the nature of what a seal does, that you're aware of that in any way prevents the kind of malware "hitching a ride" that you've testified to earlier?

HALDERMAN: No. I am not aware of any seal that could do such a thing, and seals are essentially irrelevant to that kind of malware.

STEIN ATTORNEY: And a moment ago you were asked questions about comparing ballots to the count on a machine and your answer referenced the scale of that comparison, correct? And can you tell me what you meant by scale?

HALDERMAN: It means how many ballots are being recounted. A hand count scanning a small number of ballots as in pre-election tests and comparing the machine's output to what's actually on the ballots could be defeated. That's not the same as performing a hand count of the election, which is the best method we have of determining whether a cyber-attack influenced the outcome.

STEIN ATTORNEY: And how could the smaller subset pre-election type of test be defeated as you've just said?

HALDERMAN: Malware might be programmed, for instance, not to cheat unless a large number of ballots were being counted as the number found in a typical polling place.

STEIN ATTORNEY: I have no further questions.

STATE ATTORNEY: I understand your testimony to say that the only way to know if the outcome of an election in a particular state reflects the balance is to do a hand recount; is that right? And was it your opinion that a hand recount should be conducted in every state that was predicted to be close in the 2016 general election?

HALDERMAN: Yes. I believe that a hand recount is --or other methods of determining to high statistical confidence that the physical record matches the digital record are necessary as a routine matter of election security.

MR.STATE ATTORNEY: Nothing further. Thank you.

JUDGE: What percentage of the Wisconsin polling places what would in your mind be sufficient to determine whether or not there were any concerns with the balloting process?

HALDERMAN: A larger, random sample of polling places could be sufficient, but how large would need to be calculated by statisticians, and I have not done the calculation.

JUDGE: Thank you.

STEIN ATTORNEY: Why is it that it would have to be a random sample?

HALDERMAN: If it is not a random sample, it's possible that an attack would be designed to target only counties that were likely to use a machine count. It's also possible that also much harder to estimate the number of ballots that need to be counted in a nonrandom sample that would need to be counted by hand in order to gain high statistical confidence.

STATE ATTORNEY: Are you aware of how Wisconsin selects its samples for auditing?

HALDERMAN: I understand that Wisconsin selects a random sample of a hundred poll sites which is too small for high statistical confidence. (*Note: Sample size is the smallest problem with these audits, conducted under s.7.08(6),Wis Stats. They are not conducted until after the election results have been declared final so even if they found miscounts, they could not correct them. They do not record miscounts that resulted from incorrect/hacked programming as 'errors,' if the machines counted votes as they were misprogrammed to do. Finally, there is no procedure for expanding the audit to other machines if any of the 100 machines were found to have miscounted. Detected miscounts are treated as isolated incidents.)*

JUDGE: You may step down. Thank you.

Testimony of Philip Stark, for the Stein campaign

Direct Examination

STARK: My name is Philip Bradford Stark. I'm a professor of statistics and associate dean of mathematical and physical sciences at the University of California - Berkeley.

Broadly, I work on 'uncertainty quantification' that applies to a bunch of different applications ranging from astrophysics and cosmology on one hand to elections, and nutrition, and human hearing in another direction.

Prof. Philip Stark, UC-Berkeley Statistics

I've been working in election integrity and specifically on methods to determine how accurately votes are counted. That is, to audit election results to assure that the reported winners are the winners according to the underlying ballots, how people voted.

I've been working in that area since 2007 when I served on California Secretary of State Debra Bowen's Post-Election Audit Standards Working Group. That turned into an academic research area for me.

Then working shoulder-to-shoulder with local election officials in approximately 20 different jurisdictions in California and Colorado to develop methods that were contracted to audit elections based on laws and regulations to improve election integrity and improve election audits. I've also worked with Denmark on methods to ensure the integrity and accuracy of counts. I have testified to both Houses of the California Legislature on auditing methods. My methods ended up being incorporated into laws in Colorado and California.

I've made presentations to professional organizations of elections officials including the International Association of Clerks, Recorders, Election Officials, and Treasurers, and the California Association of Clerks and Election Officials. I currently serve on the Board of Advisors of the U.S. Election Assistance Commission.

I've written a number of peer-refereed articles on election integrity including an article called Evidence-Based Elections, which was written jointly with Professor David Wagner, a computer scientist here. I've been an invited speaker or keynote speaker at a variety of conferences nationally and internationally relating to election integrity and verifiability of voting, transparency voting. I'm working with a group in Travis County, Texas, where Austin is. The group is led by Dan Wallach, computer science professor for Rice University, developing a voting system that is designed to be auditable, transparent, and who are combining cryptographic end-to-end verifiability with paper based audits, an audit trail. Let's see. What else.

Stein Attorney Debbie Greenberger

STEIN ATTORNEY GREENBERGER: Can you speak generally about any vulnerabilities that you know of about opscan computerized voting equipment?

STARK: Yes, ma'am. There are several different strategies to optically scan voter-marked ballots. There are mark-sense style optical scan systems. There are imaging-style optical scan systems. But broadly, yes.

STEIN ATTORNEY: And do you know of any errors in the tabulation of optical scan voting system results that could occur? Could you describe those?

STARK: Wisconsin is a state that considers voter intent in determining whether a ballot has been interpreted correctly by the voting system. Optical scan systems can fail to correctly ascertain voter intent for a number of different reasons ranging from problems with how they are configured, problems with how they are maintained, mechanical issues, failing to scan all of the ballots or scanning some batches of ballots more than once, mechanical problems such as mis-picks and mis-feeds or jams.

Because software cannot perfectly ascertain voter intent from various kinds of voter marks, there can be variability according to the kind of ink that the voter uses to mark the ballots, variability depending on whether the voter marked the ballot per instructions or makes a mark like circling something that should be filled in or putting an X where something should be filled in.

There can be variations in how the equipment reads ballots depending on the physical length of the ballot. I know of an instance where the printer had trimmed the ballots to an incorrect length resulting in the scanners not recording the ballots as having any votes. There are instances where the scanner has overflowed their buffers for counting and started to count backwards. There are all kinds of things that can contribute to a difference between how a human adjudicator would tally the votes on paper ballots and how an optical scan system would tally the same votes.

STEIN ATTORNEY: The margin in the Wisconsin Presidential race between the President-elect and the second place candidate was approximately 22,500 votes. Given that margin, what does that mean about what percentage of error would need to be made by the optical scan machine to affect the outcome of the Wisconsin vote?

STARK: Errors in the interpretation of less than 0.38 percent of the ballots—that's less than one percent--could result in causing a tie or a win for Secretary Clinton appear to be a win for Mr. Trump. That means that even if the vote tabulation was more than 99 percent accurate, it still could be inaccurate enough to affect the outcome of the election statistically.

STEIN ATTORNEY: Are you familiar with a recent study by Professor Walter Mebane about the Wisconsin vote? Can you explain to the Court what the study found?

STATE ATTORNEY: Your Honor, I object to this line. Professor Mebane apparently did a study. That study was reported on in the Washington Post and Dr. Stark's affidavit explains his interpretation of the Washington Post article. This is just too far removed. It's an attempt to get an expert testimony through the backdoor through a non-expert, and it's just not competent evidence.

STEIN ATTORNEY: Your Honor, first of all, that's incorrect. Professor Stark reviewed the study itself, which is also attached to his affidavit as Exhibit B, not just the Washington Post article. They're both attached. And as an expert, he can review all competent evidence. To the extent they want to cross-examine Professor Stark him on the competency of the evidence, they're welcome to, but it's certainly well within his competency as a statistician to review other peers' studies and evaluate them.

JUDGE: I'll overrule the objection. You may answer the question.

STARK: Professor Mebane is a professor of political science and statistics at the University of Michigan. He's an expert on election fraud and detecting election fraud statistically from reported election results.

This particular paper of his, a working paper, uses ward-level results from Wisconsin from the current elections. I understand that the data were current as of approximately a week ago.

He applies a battery of standard tests for suspicious election results to this ward-level data from the Wisconsin election. The tests were developed with funding from the USAID.

None of the test is comparing the reported percentages or number of votes to the share that a candidate was expected to get according to polling or anything else.

Rather, these tests look at the numbers themselves and say in situations where we count things in large numbers, we would not expect any particular digit to occur more frequently than any other in the 1's place in the count. So if you see that in the 1 's place in the count you tend to get numbers that are smaller than 5 more frequently, or you tend to get 0 or 5 less frequently than you would expect, that may be a sign that something has caused the numbers to differ from their true values.

In Professor Mebane's examination of Wisconsin ward-level election results, he found that the results from optical scan systems in smaller wards are suspicious in that, under a standard statistical model for the digit frequency of terminal digits or the next to the last or the second digit, the numbers are different than expected—by an amount that would be considered statistically significant.

The frequency of zeros and fives is surprisingly high, and the terminal digit of the count is surprisingly low. In the ward count, the terminal digit of zeros and fives in the rounded 50 percentage error of a

candidate was surprising in some of those smaller wards. There also appears to be multi-modality, meaning there's more than one most frequent digit in the distribution of those supporting some of the tests that he did.

None of this demonstrates conclusively that the totals are erroneous or that anything malicious happened. The only way to determine that conclusively is to go back to the paper records by hand and examine them. But these statistical results would be surprising under standard models for what results ought to look like, including things like the last digit of the results.

STEIN ATTORNEY: And did these suspicious, surprising results occur in opscan areas, or areas that have the other type of voting machine in Wisconsin, DRE areas?

STARK: The ones I was just mentioning are in opscan areas.

STEIN ATTORNEY: Why do you say that the only way to determine whether these suspicious results indicate that something malicious occurred is to do a hand recount?

STARK: Well, first of all, the amount of error that could have caused the pre-electoral result to differ from the reported result is very small and could easily have occurred as a result of either innocent normal errors, normal malfunction, or limitations of optical scan equipment, or as a result of some kind of bugs or errors in the software or malicious hacking of the software or systems.

So to simply put the same ballots back through the optical system and tally them again that way would not give us an answer.

An analogy for that would be someone goes to a doctor, gets a diagnosis, and says "I'd like a second opinion," and then the doctor says, "Okay, I'll tell you a second time." That's not an independent, second judgment.

To ask the system to check itself might detect certain kinds of errors, but would miss many other kinds of errors. Some of the normal errors would simply be repeated if you re-scan the same ballots—if not repeated exactly, then repeated approximately.

For example, if a voter had mis-marked a ballot by circling the vote target instead of filling in the vote target, the machine would be likely to misread it the same way both times that ballot was scanned. If two ballots were stuck together in the scan and went through together the first time, it could be likely that those same two ballots would be stuck together the second time they go through the machine. If the software in the scanner had bugs or had been hacked, it would be expected to behave the same way both times the ballots were fed through the machine.

There would be no way on the basis of a re-scan to determine whether the original results were wrong. At best, you would find out whether asking the same question twice of the same device produces the same answer.

STEIN ATTORNEY: Moving to a different area, did you see that the WEC Director has stated that they rely on the U.S. Election Assistance Commission's program of certification of election equipment? Reminding the Court that Professor Stark is on the Board of Advisors of that same U.S. Election Assistance Commission, can you please tell us your view about Wisconsin's reliance on the Election Assistance Commission's certification of election equipment?

STARK: It's probably better to use certified equipment than not at this stage of the market. But that certification is not a guarantee of election accuracy.

To use an analogy, relying on certification as insurance of the accuracy of the result would be like a brain surgeon saying I used a sterile scalpel, therefore, the patient is fine. All other things being equal, it's certainly better to use a sterile scalpel than one that isn't sterile. But if you want to know whether the operation went well, you have to look at the patient.

Similarly, it's probably better to use certified equipment than not. But if you want to know if the election went well, you have to look at the ballots. And certification is not a guarantee of accuracy.

STEIN ATTORNEY: Tell me why that is.

STARK: Well, the part of certification test that relates to tabulation accuracy amounts to taking a brand new machine, running machine-marked ballots through that machine in a laboratory, and figuring out whether the equipment is capable of tallying votes to a pre-specified level of accuracy.

In a real election, you have equipment that has been in a warehouse. It's been transported. It's some years old. It's being set up by poll workers who have varying degrees of training. It's being fed ballots that had been marked by real voters rather than perfectly marked ballots. The accuracy with which that tabulation occurs is very different in principle from the accuracy with which a brand new machine processes machine-marked ballots.

STEIN ATTORNEY: Does the certification ensure that this machine could not be vulnerable to a cyber-attack?

STARK: No, it does not.

STEIN ATTORNEY: In that same submission from the WEC Director, did you see that he spoke about Wisconsin's process of auditing election results?

STARK: Yes. I understand from his declaration that Wisconsin collects a hundred groups of ballots from different parts of the state and compares a machine count of those groups of ballots to a hand count of those groups. *(Note: This is an incorrect understanding. The ballots never leave the municipal clerks' possession. The State tells municipal clerks to hand count the ballots and to report any miscounts that cannot be explained by mis-programming or human error. The municipal clerks receive no supervision or oversight in this task.)*

STEIN ATTORNEY: And do you have a view on whether that audit ensures that the election results are accurate?

STARK: Yes. It is my opinion that it does not ensure that the election results are accurate for a number of reasons.

First of all, in the worst case, suppose that one selected a hundred batches of ballots at random from the state but that there were errors amounting to errors in 0.4 percent or .038 percent of the ballots, which is all that would be required to change the electoral outcome in Wisconsin. There could be as large as a 67 percent chance that none of those hundred batches would show any discrepancy whatsoever.

Secondly, I understand that as of the date of Mr. Haas' declaration, only six of those samples have been drawn and only four of them have been examined. The probability that you could get six perfect counts and yet still have an error rate of .04 percent or higher among all ballots is on the order of 98 percent.

Moreover, in his reference to the four batches that have been examined, he refers to them as not having any unexplained discrepancies. It doesn't really matter whether the discrepancies have an explanation or not. What matters is whether the count according to the opscan machines is equal to the count that a human doing his or her best job of inferring voter intent from the physical ballot will find.

STEIN ATTORNEY: So if I understand your testimony correctly, even if there was an error in Wisconsin's voting equipment that was large enough to effect the outcome of the election, the fact that even if there was an error large enough to effect the outcome of the election, there is a 67 percent chance that after the audit is completed, that error would not be discovered. Is that correct?

STARK: The chance could be as large as about 67 percent that every batch --every one of the hundred batches inspected would match perfectly and yet the answer is incorrect, the electoral outcome is incorrect. Based on the batches that have been examined so far, the probability could be as high as about

98 percent that those four batches would show no errors whatsoever, and yet the aggregate error in the election as a whole was large enough to change the apparent outcome.

STEIN ATTORNEY: I have nothing further.

Cross-examination

STATE ATTORNEY: On page 6 of Professor Mebane's paper, he writes "Why do small wards with opscan technology (and several other kinds of wards) have anomalies, and do the anomalies mean the reported vote counts do not accurately reflect the intentions of the electors? Given all the information we have, it is hard to say." You don't have any basis to disagree with that, right?

STARK: That's correct.

STATE ATTORNEY: Earlier in your testimony you identified a number of potential problems with opscan reading of ballots. This is not meant to be an exhaustive list, but examples are how it's maintained, mis-trimming of the ballots, scanning ballots more than once. Those are potential problems of any opscan system, right, not just Wisconsin?

STARK: Yes, sir.

STATE ATTORNEY: And you don't know how the machines in Wisconsin are maintained, right?

STARK: I have no specific knowledge. I would imagine that it varies quite a bit from jurisdiction to jurisdiction.

STATE ATTORNEY: And you're not aware of a printer mis-trimming the length of any ballots in Wisconsin?

STARK: No, sir. *(Note: A vote-altering ballot-printing mishap occurred just three months before this hearing, in Dane County, where this hearing was taking place.)*

STATE ATTORNEY: Of those types of systemic errors, there's no reason to think that they would all err in the direction of one candidate or another, is there?

STARK: For those particular errors, I can't think of a reason that they would favor one candidate rather than another. But they are haphazard in nature and it would be difficult to predict what their effect would be on the count.

STATE ATTORNEY: You gave some opinions toward the end of your testimony about the audits that Wisconsin does. You don't know the number of ballots in each batch of audited ballots in Wisconsin, do you?

STARK: No, sir.

STATE ATTORNEY: I have no further questions.

Re-direct examination

JUDGE: Do you know how many know how many wards Professor Mebane focused on? If I recall correctly, he considered a small ward to be one that had a hundred or fewer ballots cast. Do you know approximately how many wards that constituted?

STARK: I don't off the top of my head. I'm sorry.

JUDGE: Okay. And so his conclusions were related to the small wards; is that correct?

STARK: Not entirely. But the anomalies that he found were primarily in the small wards. There's one column in his table one that applies to large wards, and I'm not quite sure what the number the label none means there, but I don't recall what that means in the caption of this paper.

JUDGE: Do you think that the small wards could have added up to over 22,000 votes?

STARK: I don't know how many votes there were in all in them and so I'm not I just don't have the basis on which to answer.

JUDGE: The anomalies, if I understand looking at Table 1, were both in districts that went in favor of Mr. Trump and those that went in favor of Ms. Clinton. Is that correct?

STARK: My understanding is that according to these tests there were anomalies in districts that went for both of those candidates. Okay. Thank you.

JUDGE: I have no further questions.

STEIN ATTORNEY: Does the fact that the anomaly occurred in a ward that favored Trump or Clinton indicate whether the anomaly caused the votes to swing in favor of Trump or Clinton?

STARK: The anomaly is not itself proof that there's anything wrong with the counts at all. It just suggests that it would be prudent to examine the underlying paper records to find out what happened. The anomalies are not with respect to the margins in these wards. Rather, they're to do with the raw numbers and whether the digit frequencies appear suspicious.

JUDGE: No further questions? Okay. Thank you very much, Professor Stark.

Testimony of Ron Rivest, for the Stein Campaign

Ron Rivest, MIT Computer Science

Direct Examination

RIVEST: My full name is Ronald Linn Rivest. I'm an institute professor at the Massachusetts Institute of Technology. I do research in security broadly, including cryptography and election security. The most notable award I've received is perhaps the ACM Turing Award, an award for contributions to computer science. In this particular case it relates to the invention of the public-key cryptosystem know as RSA. The RSA cryptography is a public-key cryptosystem that's used in most web browsers these days for securing the browser connection. It involves the product of large prime numbers, and encryption is performed by performing modular exponentiation where the module is the product of prime numbers. More of my research relates to trying to detect compromises and design systems that are immune from compromises. Most of the work on detection of compromises has to do with auditing technology.

STEIN ATTORNEY BRINCKERHOFF: Professor Rivest, are you familiar with a term called "software independence"?

RIVEST: Yes. That's a term that I coined together with my coauthor Jonathan Wack. It's very similar to the notion of auditability. It means that a software, a voting system in particular, is software independent if an undetected change in the software cannot cause an undetectable change in the election outcome.

It means that it's more auditable. If it's software independent, it means you're not in a software-dependent state. In a software-dependent state, you basically have to trust the software.

STEIN ATTORNEY: In American elections using scanning technology, is that an example of software independence or dependence?

RIVEST: That's an example of software independence because you have the opportunity to detect if the scanner was misbehaving by examining the paper ballots.

STEIN ATTORNEY: Aside from examining the paper ballots, is there any other way to detect whether or not there is a problem with the software that is used to drive the machinery of the election?

RIVEST: Well, there are other methods that might be used, but they tend to be very complicated, imperfect, expensive, and only partial. For example, one could try to examine a code that was running on the machine, however, most machines, voting machines, don't even have the ability to examine the code. It's loaded onto the machine. You don't know what software is actually controlling the machine.

STEIN ATTORNEY: You're saying that when it comes to voting machine software --and let's be specific here and talk about specifically the scanning kind of technology and software --are you saying that there's no way to independently verify even what software is running on those machines?

RIVEST: That's correct. I mean, you're putting trust in the vendor that when you load the software onto the machine that software is what is actually running. It could be the case that the software on the machine is some other software that was installed some other way and the software that you think is loaded is, in fact, ignored.

STEIN ATTORNEY: And do you have an opinion in general about how vulnerable opscan technology is as it's used currently in American elections?

RIVEST: I have not directly investigated them. These machines are computers. They tend to be rather simple from a security viewpoint. They can be compromised. So their vulnerability is noticeable. Whether they're actually being compromised in the field, I don't have any evidence.

STEIN ATTORNEY: Are there any other methods besides recounting the hand paper ballots that you're aware of that could be used to detect whether or not the election systems were compromised by malicious intrusion?

RIVEST: I don't know of any. The idea, for example, of rerunning all of the ballots through the same machines certainly fails to detect whether those machines have been compromised. Because if they're faulty, if they're malicious, and they sort of preplanned errors or changes, the rerunning of the data through those machines, one would expect to get the same results out of those machines again, erroneous results.

STEIN ATTORNEY: You're familiar, I believe, with the fact that some of the counties intend to rerun these ballots through machines and others will not. Do you have an opinion as to which one of those methods is likely to be the most reliable and reflective of the actual votes cast on Election Day?

RIVEST: I would strongly favor a hand count of the ballots themselves, because that reflects the will of the voters without the potential corruption of any errors in the programming of the machines that are doing the scanning.

STEIN ATTORNEY: Okay. And I take it we've mentioned malicious intrusions and errors. Am I correct that both of those kinds of problems can result in vote tabulations and tallies being inaccurate?

RIVEST: That's correct. I mean, it need not be a malicious intrusion that would cause an error. It may just be a mis-programming that causes votes for A to be counted for B and vice versa.

STEIN ATTORNEY: I understand that you are a supporter of voting systems that create a voter-completed record of the vote; is that right?

RIVEST: Yes. A voter-verified paper audit trail. If the only official record of the voters' choices are only electronic bits somewhere in the guts of a machine, the voter has no real ability to tell whether those bits are being accurately set to record his choices.

STEIN ATTORNEY: And do you have an opinion of how reliable you would consider the vote to be in Wisconsin if all of the ballots were examined by hand?

RIVEST: The hand count is typically viewed as the gold standard for accuracy if it's done well. You have a number of people looking at each ballot and checking for voter intent and recording it multiple ways. So this would be the highest, not to say that it's perfect, but it's the best we know how to do.

STEIN ATTORNEY: Are you familiar with a term called "script kiddie"? Can you tell me what that is, please?

RIVEST: That's a term that relates more to the eighties and nineties perhaps when the hackers of the computer system were perhaps high school kids who didn't know really anything about security and attacked systems merely by copying a script from a website somewhere and applying it against another website that you wish to attack.

STEIN ATTORNEY: And do you have any view or opinion about whether or not the Wisconsin election system is vulnerable to some kind of intrusion by script kiddie?

RIVEST: I wouldn't think they would be.

STEIN ATTORNEY: Okay. And do you have any opinion or view about whether the Wisconsin election system is vulnerable to intrusion or attack by a more sophisticated state-sponsored, potentially, hackers?

RIVEST: We've learned over the last decade or so that almost any system can be compromised by an adversary who's skillful and persistent and determined. And I've seen with my own company, RSA Security, that various break-ins are possible, whether they're by the Chinese or others. We've seen it with military establishments.

And when you talk about security for the Wisconsin voting system, you should keep in mind not only the servers and voting systems of the election system themselves but also those of the vendors and distributors that are supplying the software.

Think not only of what happens on Election Day, but what happens in the months and years beforehand. If a foreign power were to gain the passwords of all of the election officials of the state, *(Note: or even just Milwaukee County)* how secure would the system be then? That could be something that could have happened well before Election Day.

STEIN ATTORNEY: So do you have any confidence based on your knowledge of computer science that the Wisconsin election this year, the Presidential election, was not compromised in some fashion by some kind of foreign malicious attack?

RIVEST: To be confident that the system was not attacked, I would look for evidence produced by examination by hand of the paper ballots. That would be the level of assurance that I would look for. And so this recount with a recount by hand would provide that assurance. Absent that, the level of assurance is beneath my standards.

STEIN ATTORNEY: Thank you, Professor Rivest. I don't have any further questions.

Cross-examination

STATE ATTORNEY: I believe you just testified that almost any system like the scanning system you've been discussing could potentially be compromised, right? So that analysis is in no way specific to voting procedures in Wisconsin, right?

RIVEST: That's correct. The equipment that's used in Wisconsin is, by and large, rather generic, in fact, rather primitive in some regards compared to security systems of many computers. But, you're right. It's more of a generic system that the computer systems in general tend to be fragile and don't have the kind of security that we'd like to see them have.

STATE ATTORNEY: Is it fair to say that you have a mistrust of opscanning system in elections?

RIVEST: I like optical scan systems. They're a useful tool. And I think that having a quick count by an optical scan system is good. I think that generally they're pretty reliable. And when they're not tampered with, they're pretty accurate. But, you know, they're not perfect. Statistical audit of the system is just good practice and should be followed to verify that they're accurate.

STATE ATTORNEY: Are you aware of any evidence that malicious software or other compromises have been installed in Wisconsin voting machines?

RIVEST: What sort of evidence would you imagine that it might have? I don't quite understand how I would be in a position to answer that.

STATE ATTORNEY: Paragraph 33 of your affidavit says, "I should emphasize that I have no particular evidence of manipulation or tampering of the ballots or the results of the 2016 U.S. Presidential election." Is that accurate?

RIVEST: That's correct.

Testimony of Michael Haas, for the Wisconsin Elections Commission

Michael Haas, Director
Wis. Elections Commission

Direct examination

HAAS: My name is Michael Haas. I'm the administrator of the Wisconsin Elections Commission, which is the state agency that administers and enforces election laws in Wisconsin.

I oversee our staff of approximately 30 positions. We attempt to administer and implement and interpret any new legislation dealing with elections.

A few of our chief responsibilities are to train and provide guidance to local clerks, county clerks and municipal clerks, who conduct elections. We publish or issue guidance in a variety of forms. We conduct training, webinars, and in-person training.

Our staff also reviews nomination papers or election petitions that are filed at the State level. We develop and maintain the statewide voter registration system, which is a database containing all the States' registered voters.

Our agency also tests voting equipment, approves voting equipment for use in the state of Wisconsin. Our tasks are to work with clerks, work with candidates, work with the legislature, state officials, other agencies, work with federal and state agencies on securing election systems. We also certify election results.

STATE ATTORNEY: What types of equipment does the state of Wisconsin use for voting?

HAAS: Wisconsin is one of the most, or the most, decentralized election systems in the country. We have 1,854 municipalities responsible for purchasing the voting equipment used in their municipality, typically purchased in coordination with the county clerk. And there's a variety --a handful of different types of voting equipment used in the state. But generally speaking, it's optical scan tabulating equipment and electronic equipment electronic tabulating equipment or DREs.

A DRE basically is touchscreen equipment. And so a voter can go in and, instead of marking votes on a paper ballot, can touch a computer screen. There is a voter-verifiable paper audit trail where the votes are reflected or printed, basically like a cash register receipt spool. The voter can verify that the votes have been recorded properly by the touchscreen equipment. That equipment has a second spool of paper that also records the identical votes, and that is the basis for any recount of DRE-cast votes is done using that paper spool, basically a hand count of that recorded vote.

With the optical scan equipment, a voter marks votes on a paper ballot, and inserts the ballot into the tabulating equipment. Probably roughly 85 percent of ballots in Wisconsin are tallied using optical scan equipment, 10 to 11 percent are cast using the DREs, and the remainder are hand counted ballots.

STATE ATTORNEY: What does WEC do to make sure that votes are recorded as they are cast?

HAAS: The equipment is tested, approved, and certified at various levels. At the federal level, it is tested by independent testing labs that are certified by the U.S. Elections Assistance Commission. Those tests and reports are submitted to the EAC, which ultimate decides whether or not to certify the equipment for technical standards, security standards, programming, things like that.

And then at that point a voting equipment manufacturer can come to the state of Wisconsin, to submit an application for approval. Our agency conducts a functional test of the equipment to ensure that the equipment will do what our statutes require.

We will create test decks of ballots and run those ballots through the equipment. We mark the ballots in a variety of ways, one of the goals being to push the envelope with the equipment. See if the equipment will tally a vote inaccurately if we can try to trick the equipment, essentially.

And then the equipment is also often taken out on the road in the field and tested in counties with municipalities in more real world conditions.

A report is then prepared for our Commission. If the equipment is approved, it is normally approved with a number of conditions designed to ensure that the equipment will continue on an ongoing basis to comply with the statutes and how it tabulates votes.

Once the equipment is approved for use by our agency, municipalities may purchase it.

STATE ATTORNEY: So, is there any equipment in use in Wisconsin today that hasn't been both federally tested and approved and field tested and reported on by the Elections Commission?

HAAS: No, with the exception of some components of the equipment. In a couple of cases, there have been components of equipment that were not certified by the EAC and Wisconsin as a statute allowing for approval even without certification. And with those components, the underlying system or machine had been certified by the EAC and our agency.

STATE ATTORNEY: Okay. So there's no equipment being used now that has not been field tested by the Elections Commission?

HAAS: Correct.

STATE ATTORNEY: So, what happens with the equipment before Election Day to ensure that the results are going to be reliable?

HAAS: The equipment, as I said, it needs to undergo a public test within 10 days of Election Day, and so each municipal clerk will provide public notice of the public test, the public is invited to come and observe the test. In those tests, a deck of test ballots is created so you have essentially a predetermined tally. You know how those ballots should be tallied. They are run through the equipment to ensure that the equipment is accurately tabulating those ballots. The equipment is programmed either by the county clerk or more often by a voting equipment, manufacturer, or vendor representative that will assist the county clerk in ensuring that the equipment is programmed accurately for that particular election.

STATE ATTORNEY: If a piece of equipment doesn't pass that test, is it used on Election Day?

HAAS: No. *(Note: There are two problems with this answer. First, if the municipal clerk follows WEC instructions, the equipment is used on Election Day, but the set-up error is corrected. The underlying programming remains untouched. Second, WEC does not oversee these pre-election tests. So Haas should have answered more along the lines of "I believe that to be so, but I have no direct knowledge about whether the municipal clerks find problems, or what they do when they find them")*

STATE ATTORNEY: What happens to the equipment after that test is run?

HAAS: The equipment is secured by the municipal clerk until Election Day. Locked up, so that unauthorized individuals do not have access to it. On Election Day then, there's a protocol for the election inspectors or the poll workers to ensure that there are no votes tallied before the polls are opened, before real ballots are inserted into the tabulating equipment.

STATE ATTORNEY: Are the machines ever connected to the Internet before Election Day?

HAAS: No, the machines are not connected.

STEIN ATTORNEY: Objection. We have not established what machines we're talking about. *(Note: The other computers might be the county's central election-management computer, or any of the computers used by the vendors or servicing companies.)*

STATE ATTORNEY: Voting election tabulation machines in the state of Wisconsin.

HAAS: They are not connected to the Internet on Election Day.

STATE ATTORNEY: How are votes tallied and counted after Election Day in Wisconsin?

HAAS: Unofficial results are tallied after the polls close at 8 o'clock.

STATE ATTORNEY: Who tallies the official results? Tell us about that process.

HAAS: In the couple of weeks after the election, the counties will hold their official canvass where their canvass board will meet, they will review the election materials, review the results, reconcile the numbers of voters with the number of ballots, and then they will produce a certified canvass.

Those official canvass results are transmitted electronically into the State's canvass reporting system. The canvass board members also sign a certification, which is transmitted to our office.

STATE ATTORNEY: When you say sign one, what is that document? I mean, is it something you get in paper?

HAAS: It's typically faxed.

STATE ATTORNEY: What steps are taken after Election Day to verify that the machines were working correctly?

HAAS: Under Wisconsin statutes, after every November general election, there is a post-election voting equipment audit where we randomly select a number of reporting units and direct municipalities to conduct an audit—a hand count—of ballots.

The purpose of that is not necessarily to verify the results. It's to verify that the voting equipment is counting the ballots properly. *(Note: This is a distinction most casual observers miss. The Wisconsin audits are designed to check the accuracy of only the hardware. The WEC considers misprogrammed software to be a human error, not a machine error, and they do not believe the statute requires them to audit for software problems. If miscounts are noticed that can be explained by misprogrammed software, WEC instructs the municipalities not to report them as errors.)*

STATE ATTORNEY: How are the audit locations selected?

HAAS: They're selected by random. We have come up with a computer program to randomly select those reporting units. We have a spreadsheet listing every reporting unit for that election and the program then will randomize that list. We start out taking the first hundred reporting units selected and then we adjust it for two reasons. One is to ensure that every type of voting equipment hardware is represented in the audit and is audited at each general election.

And this year we tweaked the procedures so that no municipality was required to audit more than two reporting units.

STATE ATTORNEY: Walk us through the mechanics of an audit. What happens at the machine?

HAAS: Well, two human tabulators will conduct a hand count.

STATE ATTORNEY: Is that audit being done for the 2016 fall election right now?

HAAS: It was ordered. We have currently suspended it in light of the pending recount. A handful of municipalities conducted the audit before we certified the results. But as of Monday, we advised the remaining municipal clerks to suspend the audit in light of the recount and we would reevaluate whether it would be initiated again after the recount. A recount and the audit have separate purposes. The purpose of the audits is not necessarily to verify the results. A recount reviews many more parts of the election process than the audit.

STATE ATTORNEY: What were the results of the portions of the audit that was completed before it was suspended?

HAAS: We received, I believe, six audits just in the last week. We haven't had time to extensively review them. On a really quick review they show that there were no anomalies. In other words, the voting equipment accurately counted all of the ballots.

STATE ATTORNEY: Now, your declaration says that the audit found no unexplained discrepancies. Could you expand on that?

HAAS: That's probably just terminology. I think in one of the four that we briefly examined, there was a discrepancy in the number of ballots that were tallied for write-in candidates that the equipment would not have counted. And so the clerk determined that the two individuals conducting the audit were short two ballots, essentially. But the clerk was convinced that she had a reasonable explanation for why there was that discrepancy. Again, that was not a discrepancy in how the voting equipment counted the ballots.

STATE ATTORNEY: Do you know of any discrepancies in any of the vote counting for the November 2016 general election?

HAAS: That's a broad question. We saw some errors that were made on election night, for the unofficial results. There was one notable case in Outagamie County that received some attention and there was an explanation for why that discrepancy appeared.

STATE ATTORNEY: Let's talk a little bit about the recount process. When will the recount start?

HAAS: It’s scheduled to start 9 AM Thursday. The canvass boards will again assemble. The county clerk is essentially in charge of managing the process, hiring as many tabulators, individuals as they feel that they need.

They have a number of preliminary steps to reconcile poll lists and other election materials, absentee ballots, envelopes, things like that.

STATE ATTORNEY: For each of the three categories of the machines that you discussed at the beginning, tell us how the recount is done mechanically, logistically.

HAAS: The votes are tallied either by hand count, in the case of paper ballots that were originally hand counted; or a hand count of the audit trail from the touchscreen machines; or they will use the optical scan equipment, or a combination of those.

STATE ATTORNEY: I want to stop there to clarify that. So there are three methods of initial accounting. Am I correct that two of those are hand recounted as a matter of course?

HAAS: The ones that were originally hand-counted, and the ballots printed on the audit trail by the DREs. Correct.

STATE ATTORNEY: For the third category, who decides whether to hand count or optically scan?

HAAS: It's a decision of the canvass board in each county. In a survey we conducted so far, approximately 19 counties indicated that they would use tabulating equipment for some or all of their ballots. Those were based on responses from the county clerk who would be making that recommendation to the canvass board that would make the ultimate decision.

STATE ATTORNEY: Why do the local authorities get to choose?

HAAS: That's what the state statute permits.

HAAS: Based on your expertise and experience, do you know why a municipality might choose hand counting as opposed to mechanical counting or vice versa?

HAAS: It could be a variety of reasons. County clerks have different viewpoints on it. So, generally speaking, we would expect that the more populous counties would lean towards using tabulating equipment. Dane County, our second most populous county, intends to hand count their ballots.

Hand counting generally is going to require more workers, more individuals hand counting those ballots. One county indicated to us that they would need 60 tabulators for a hand count, versus 20 if they were using tabulating equipment.

There's a cost of programming the tabulating equipment, which can be avoided if the ballots are hand counted.

There are also time considerations. Because each ballot needs to be manually examined anyway before it is put into the tabulating equipment, the time savings in using tabulating equipment may not be as significant, depending on the number of ballots.

STATE ATTORNEY: In your interactions with clerks, have they expressed an accuracy difference or concern between the two methods?

HAAS: No.

STATE ATTORNEY: Do you know if some clerks have already chosen a method of recount that they plan to use?

HAAS: Yes. Many of the clerks have chosen what they expect and will recommend to the canvass boards. As I said, ultimately, it's up to each canvass board.

STATE ATTORNEY: Counties that intend to use tabulating equipment—are they already in the process of lining up the programming they need to again program and test the tabulating equipment before they can use it at the recount?

HAAS: Correct.

STATE ATTORNEY: And when does the recount need to be completed?

HAAS: Our Commission met yesterday and directed that the recount needs to be finished by 8 PM on December 12th. There are some considerations under federal law about a deadline of either December 13th or possibly at the latest December 19th in order to ensure that Wisconsin's electoral votes are honored by Congress.

STATE ATTORNEY: Who can observe a recount?

HAAS: Members of the public, and specifically representatives of each candidate who ran in the contest that is being recounted. Each candidate has a right to have representatives at the recount in order to observe the process and raise any objections or challenges to either the ballots or the procedures.

They can look at every ballot. They can look at the materials. They're not supposed to be touching the materials but they can be looking at every vote. They can make their own tally if they want. And they can,

as I said, raise any challenges in the case of a hand tally whether or not they agree with how the vote is being counted.

STATE ATTORNEY: Are you aware of any evidence at all that voting equipment in the state of Wisconsin malfunctioned or was tampered with in a way that might affect the results of the November 2016 general election?

HAAS: No. Malfunction's a broad word, though. Voting equipment malfunction is not unusual on Election Day. There might have to be a maintenance person that comes to repair it. But as far as malfunctions that affect ultimately the official results, the answer is no.

STATE ATTORNEY: Are you aware of any mistakes in the canvassing and vote counting process that affected the results of that election?

HAAS: There was a typo in one of the official certifications that would need to be corrected if it stood for the Presidential election, but that has been fixed. But I'm not aware of any mistake in the canvassing process that occurred due to the use of tabulating equipment.

MR.STATE ATTORNEY: I have no further questions.

Cross examination

STEIN ATTORNEY: You just testified that Wisconsin municipalities purchase the voting equipment from private vendors, correct?

HAAS: Correct. I'm not aware of any public vendors that sell voting equipment.

STEIN ATTORNEY: And when the municipalities purchase the equipment from private vendors, the equipment comes pre-equipped with software to enable the equipment to scan and tabulate the ballot, correct?

HAAS: I'm actually not sure what comes with the delivery. I wouldn't be surprised if that's the case. It needs to operate.

STEIN ATTORNEY: So you certainly couldn't rebut what our experts just testified to that it came with that software technology, correct?

HAAS: Right.

STEIN ATTORNEY: And it is in fact true that when the equipment comes from the private vendor, it already has the capability to scan ballots and tabulate results, right?

HAAS: It has the capability to do that assuming that it's programmed accurately for the specific election.

STEIN ATTORNEY: And you testified that when a municipality in Wisconsin is looking to purchase new computer voting technology, they do field testing, correct?

HAAS: The State does the testing. When we are doing the testing, often we will --we know which municipalities or counties are interested in that equipment. So as part of our field testing, we will try to arrange to go to those areas, but that does not mean that every municipality is involved in that testing.

STEIN ATTORNEY: But as part of your field testing, it's fair to say that you don't do a forensic computer audit of the equipment, correct? And as part of your field testing, you don't review the source code of the equipment, correct?

HAAS: Yes.

STEIN ATTORNEY: you don't have a computer specialist or computer forensic scientist on staff with your agency, correct?

HAAS: Correct.

STEIN ATTORNEY: So you have no way of assuring that at the time that the municipality takes delivery on the equipment, it didn't already have malware or a bug in it, correct?

HAAS: Our agency does not inspect the equipment when it's delivered at the municipality, so no.

STEIN ATTORNEY: And you said that a part of your field testing, you do testing of stacks of ballots, correct? And the hope is that because those test samples are accurate, the ultimate vote tabulation on Election Day will also be accurate, right?

HAAS: That testing, along with the other measures as I indicated, correct.

STEIN ATTORNEY: Are you aware of the controversy that has occurred with the Volkswagen cars where their admission testing was accurate for the testing stage but the computer software knew to distinguish between testing and actual use?

HAAS: Not specifically, no.

STEIN ATTORNEY: You said that the public is invited to the pre-election voting-machine tests. But they are not permitted to inspect the software in the machine at that stage, correct? They're not entitled to open the machine up at all, correct?

HAAS: Right.

STEIN ATTORNEY: And they can't do a forensic audit, correct? And they can't do a review of the source code, correct?

HAAS: Correct.

STEIN ATTORNEY: You also testified that most often the equipment is programed by a private vendor for each election specifically, correct? And that private vendor creates the ballot software in their own offices, correct?

HAAS: I would assume so.

STEIN ATTORNEY: And they create that software on computers, correct?

HAAS: Again, I would assume so.

STEIN ATTORNEY: And you have no way of knowing whether those computers are connected to the Internet, correct?

HAAS: Correct.

STEIN ATTORNEY: And it's fair to say that it's likely that those computers are connected to the Internet, right?

HAAS: I don't know.

STEIN ATTORNEY: You've never required that your private vendors keep their computers not connected to the Internet, correct?

HAAS: The State does not. You're correct.

STEIN ATTORNEY: And who the private vendors are that contract with the municipalities in Wisconsin is public information, correct? That's information that somebody who was interested in a cyber-attack could determine, correct?

HAAS: If they go to our website, sure.

STEIN ATTORNEY: The ballot software is placed onto a form of removable media; is that accurate? And that removable media is at some point inserted into the voting machine before the election, right?

HAAS: Right.

STEIN ATTORNEY: But the software gets onto the removable media by being connected to an actual computer, right? And that actual computer is located in a private vendor's office, correct?

HAAS: Fair enough.

STEIN ATTORNEY: And you said that you made two adjustments to the number of voting machines chosen for the post-election audits. Is it fair to say that you do not adjust for the spread of the election? So even in an election that was very close like Wisconsin's was this year, you don't do an audit of a larger number of municipalities, correct?

HAAS: Correct.

STEIN ATTORNEY: Professor Stark testified that there was a 67 percent chance that the audit's sample size would not be sufficient to detect an incorrect outcome. Is it fair to say that the Commission has not retained its own statistician to determine how large of an audit would be necessary to ensure accuracy of the audit? And that you yourself and no one in the Commission has that statistical knowledge base? correct?

HAAS: Correct.

STEIN ATTORNEY: Professor Rivest also testified that a hand recount is the gold standard. You don't disagree that a hand recount would be the gold standard to determine the integrity of an election, do you?

HAAS: I guess it depends what the definition of a gold standard is. A hand count, ideally, if you have all the time and all the resources. I think many election inspectors would love to use a hand count. But that is not to say that that diminishes the quality of using tabulating equipment.

STEIN ATTORNEY: In Wisconsin's own audit, you require a hand count, right?

HAAS: The purpose of the audit is to determine whether the voting equipment is working properly and so we use a hand count to do that.

STEIN ATTORNEY: When you were asked about anomalies in the election that occurred this year, is it fair to say that you testified that as I understand it over 5,000 votes were discovered to be mistakenly attributed to President-elect Trump that in fact were never cast?

HAAS: I don't think I testified about 5,000 votes.

STEIN ATTORNEY: Is it fair to say that there was a mistake in the vote tabulation in Wisconsin such that President-elect Trump was given over 5,000 votes more than he was ultimately entitled to? *(Note: The known election-night errors in the unofficial results were not electronic vote-tabulation errors, but were human-error reporting errors of the type that routinely gets made by the temporary staff who run elections, and routinely corrected in the canvass.)*

HAAS: You mean the unofficial results compared to the official results?

STEIN ATTORNEY: Correct. So on election night the unofficial results showed that there was reportedly in the media about a 27,000 vote difference.

HAAS: Those are not results that we audited or reviewed. It was reported in the media based on what the counties had reported. The official results show a difference of 22,177 votes. I have no idea if the media made a math error or if there were errors made at the local level in reporting results. Our elections are based on the official results, not unofficial results, media reports, or exit polls.

STEIN ATTORNEY: Turning to the recount that will start on Thursday, as I understand your testimony, no county has made the ultimate decision about whether it's going to do a hand recount or an automatic recount, correct?

HAAS: The formal decision is made by the county canvass board. I think in most if not all cases, the canvass board follows the lead of the clerk who has probably conducted audits in the past and has a

preferred method. But the formal decision will be made by each county at its initial canvass board meeting.

STEIN ATTORNEY: And they have full discretion to ignore the clerk, correct?

HAAS: Yes

STEIN ATTORNEY: The election supervisor Ross Hein made a statement on November 25th to the county clerks that a hand count may not be as time-consuming as one may think. You agree with that, right?

HAAS: It's a pretty general statement I can agree with depending on who is thinking it, yes.

STEIN ATTORNEY: Hein pointed out that there are advantages to a hand count because --and I'm quoting here --it avoids pretesting of the equipment and reprogramming of memory devices. That's accurate too, right?

HAAS: That was one of the trade-offs I referred to, correct.

STEIN ATTORNEY: And you spoke about cost as one of the trade-offs, right? But under Wisconsin recount procedures, the candidate who petitions for the recount is required to absorb all the cost, correct? And so in that situation there would be no cost to the public for the hand recount, no additional cost to the public from a hand recount as compared to from a manual recount, correct?

HAAS: I would say there's no monetary cost. There's certainly a significant cost in organization, scheduling, recruiting, poll workers. We talked about the difference, significant difference in the number of individuals that you need to have. And we have 12 days to conduct a recount.

STEIN ATTORNEY: A number of county clerks have recommended that their counties do a hand recount, correct? And that includes one of the most populous counties in the state, correct?

HAAS: Yes.

STEIN ATTORNEY: I have nothing further.

Redirect examination

CLINTON ATTORNEY KAUL: Just briefly following up on the Ross Hein statement, that's a statement that you approved, correct?

HAAS: I did not pre-approve it, but I don't disagree with it.

CLINTON ATTORNEY: And you were hoping the counties would do a hand recount, correct?

HAAS: No.

CLINTON ATTORNEY: That communication specifically mentioned that the Stein campaign had asked for a hand recount. And as discussed, it mentioned that a hand recount may not be as time consuming as people might think? And it indicated that was based on discussions with Wisconsin election officials over the years, correct?

HAAS: It's a subjective statement. As far as it goes, would say it's accurate.

CLINTON ATTORNEY: You mentioned a deadline, I think what's known as the safe harbor date, right, when Wisconsin must have its electoral votes determined if they are to be counted. And you mentioned you weren't exactly sure what that date was?

HAAS: No, I didn't say that. The safe harbor date is December 13th. The uncertainty is what would really be the practical effect of the recount not being completed by December 13th.

CLINTON ATTORNEY: Now, Dane County is the one that's doing the hand recount of its optical scan ballots, the big county you were referring to, right?

HAAS: That's my understanding based on what they've told us.

CLINTON ATTORNEY: And Dane County is the second largest county in the state, by population and vote total?

HAAS: Yes.

CLINTON ATTORNEY: And has Dane County expressed to you that it has any concerns about completing its recount in time?

HAAS: I have not talked to Dane County representatives about the timing. The Dane County clerk doesn't always let us know his feelings about the timing of different procedures.

CLINTON ATTORNEY: Are you aware that in 2010 Minnesota conducted a recount of the Governor's race? And that was a statewide hand recount that was completed in five days?

HAAS: I think that's what I read, yes.

CLINTON ATTORNEY: You don't have any reason to dispute that?

HAAS: No.

CLINTON ATTORNEY: And you would agree that Wisconsin can do things as well as Minnesota, right?

HAAS: Absolutely. Except we can't seem to beat them in the voter turnout percentage.

CLINTON ATTORNEY: Did you review the discussion in Secretary Clinton's brief about problems that have occurred with optical scan machines?

HAAS: No.

CLINTON ATTORNEY: Are you aware of problems that optical scan machines had in Iowa?

HAAS: No.

CLINTON ATTORNEY: How about in Florida in 2012?

HAAS: Not specifically.

CLINTON ATTORNEY: You were at the predecessor agency, the GAB, in 2011 when the State Supreme recount took place, right? And in that election, the GAB actually sought an order from the Dane County Circuit Court that would permit to hand count some optical scan ballots, right? Why was that?

HAAS: Because of a shortage of the memory devices that would need to be available for that equipment for the recount.

CLINTON ATTORNEY: And there was a concern that the data on the system would be erased if a hand recount was not done, correct?

HAAS: If the same memory devices were used as at the election, yes.

CLINTON ATTORNEY: And that issue was discovered during the course of the recount, right?

HAAS: Might have been as we were preparing for the recount. I don't remember exactly when, but at some point that issue came to light.

CLINTON ATTORNEY: But that's not an issue that the GAB was aware of prior to the recount, correct? Or prior to the process of preparing for the recount at least.

HAAS: Right. I mean, I think we know in general that if you in a short period of time need to come up with a large number of memory devices that that could be a challenge. But once the recount was requested, that became more of a priority issue.

CLINTON ATTORNEY: And you mentioned before that every member of the public has the right to inspect ballots during the recount process before they're run through the machines?

HAAS: Right.

CLINTON ATTORNEY: So an organization potentially could try to replicate a hand recount by looking at every ballot and tallying them, right?

HAAS: Right.

CLINTON ATTORNEY: And if that were to happen, that would slow the process considerably, correct?

HAAS: I guess it depends on how quick they are in marking down the hand tallies.

CLINTON ATTORNEY: But if an organization were to go ballot by ballot, that would actually be much slower than just a regular hand recount, right? That is, if an organization were only interested in doing so if there was otherwise going to be a machine recount, it would slow the process, right?

HAAS: If that was their wishes. They would have the same rights either way.

CLINTON ATTORNEY: You mentioned before that the State does an audit to determine if the tallies on the voting machines were accurate. And you said that's why they do a hand count, right?

HAAS: Right.

CLINTON ATTORNEY: The purpose of a recount is the same—to determine if the tallies were accurate, right?

HAAS: That's one of the purposes. One of the distinctions is that the audit is not auditing ballots that are hand counted and so it is not tallying up the total votes in a particular reporting unit.

CLINTON ATTORNEY: How does that work?

HAAS: They are testing the optical scan equipment to see if it worked accurately. They have the two individuals who are conducting a hand count of the votes that were tabulated by the voting equipment.

CLINTON ATTORNEY: So it's the same thing that we'd be talking about if there was a hand recount of the optical scan ballots, right?

HAAS: Correct.

CLINTON ATTORNEY: Those audits are not done by putting the ballots back through the optical scan machine? Because that would defeat the purposes of the audit?

HAAS: Right.

CLINTON ATTORNEY: No further questions.

JUDGE: Thank you. Any further questions?

STATE ATTORNEY: Are the vote tabulation machines that were in effect for the most recent fall election, were they all brand new?

HAAS: Many are old.

STATE ATTORNEY: Were any purchased before the candidates for that election were known?

HAAS: Absolutely.

STATE ATTORNEY: Do you know of any hacks or malware attacks or malware affecting any of the producers of the Wisconsin election counting equipment? Do you know if any of these manufacturers, sellers, programmers of the equipment have any indication of any attack, malware, hacking, anything 1ike that?

HAAS: We have not been informed of anything like that.

STATE ATTORNEY: Are the optical scan counters reprogrammed for each election?

HAAS: Yes.

STATE ATTORNEY: And the manufacturers are required to certify to municipal clerks that the software that is being used is what was certified and approved both at the Federal and State level. *(Note: But no one ever checks.)*

HAAS: Yes.

STATE ATTORNEY: So, programming from previous elections could not alter the results of later elections with different ballots; is that right?

HAAS: Correct. *(Note: Haas already said he is not a computer expert, and he is wrong that malware inserted before previous elections could not affect a current election.)*

MR.STATE ATTORNEY: Nothing further.

JUDGE: Thank you. Any further questions?

STEIN ATTORNEY: You testified that a removable media device is inserted into the voting machines. This applies to both old and new machines, right?

HAAS: Yes.

STEIN ATTORNEY: And that removable media device is attached to an external computer at a private vendor to get the information to then be imputed into the voting machine, right?

HAAS: It's the vendor's programming, yes.

STEIN ATTORNEY: And that removable media device that's programmed by the vendors is after the candidates are known, right? By definition it's after because it's putting on there which candidates are going to be on the ballot, right?

HAAS: Yes, after our agency certifies the candidates who are on the ballot, that's when the equipment is programmed -- or the media devices are programmed.

STEIN ATTORNEY: And that's when they're programmed by a third party vendor for which you have no idea what security computer protocols they have, correct?

HAAS: I do not know specifically what protocols they have in effect.

STEIN ATTORNEY: I have nothing further.

JUDGE: Any further questions? If you don't mind, I have a few questions. You talked about the issue regarding the memory devices and the prior recount. How is that problem fixed for this election or will be fixed for this recount?

HAAS: Well, the touchscreen equipment will be hand counted. Those ballots will be hand counted. I don't recall specifically what the equipment was in 2011 that had the shortage of the memory devices.

JUDGE: But is that an issue in this election?

HAAS: No.

JUDGE: You also told me or testified that there's a test deck of ballots for the machines. How big of a deck are we talking about?

HAAS: I'm guessing a hundred. I don't know specifically. *(Note: He has to guess because WEC does not oversee the municipal clerks' voting-machine tests. In a series of observations by the Wisconsin Election Integrity of voting-machine tests conducted in various municipalities in 2014 and 2015, no observer saw*

a test deck of more than 30. One municipality used a test 'deck' of only one ballot. However, even a test deck of 100 does not meet industry standards for a valid logic and accuracy test.)

JUDGE: Okay. How often you also testified that you do these tests to make sure the equipment hasn't failed. How often has the equipment failed the test?

HAAS: Well, if there's a problem at the public test before an election, then the clerk is required to contact the vendor and make sure that the equipment is reprogrammed or whatever malfunction is fixed, and then it needs to be tested again. If it does not pass, it's taken out of service for that election. *(Note: WEC has no direct knowledge about whether these requirements are fulfilled. Both the Medford and Stoughton miscounts are evidence that they are at least occasionally violated.)*

JUDGE: Do you have any experience as to how often that occurs?

HAAS: We hear sort of anecdotally that it occurs occasionally. I don't know statistically how often.

JUDGE: You also said that the machines are not connected to the Internet at the time of the election. Are they ever connected to the Internet?

HAAS: The results could be transferred in a number of different ways: by phone, in person, over a modem, over the telephone. Some of the newer equipment does have modems that operate using wireless Internet.

JUDGE: And so after the polls close, then when those unofficial results are transmitted, in some cases they could be transmitted.

HAAS: That instantaneous transaction would be conducted over the Internet.

JUDGE: And how --what percentage, if you know, of the machines transmit information that way?

HAAS: I don't know. It's only in the new equipment, so probably not a large percentage of the overall numbers, amount of equipment in the state.

JUDGE: You indicated that the ballots were inspected before they're fed into the machines for the recount; is that correct? Explain to me what they're inspected for.

HAAS: Well, the two tabulators, they're looking at each ballot. They will decide whether they agree or disagree on how the ballots should be counted if they are doing a hand tally. If they're looking at it for the optical scan equipment, they're just essentially inspecting it to see if they detect any issue with the ballot or how it might be tabulated by the equipment.

JUDGE: If they detect an issue with the ballot, what do they do with it?

HAAS: It may be set aside for the canvass board to determine whether or not --or how it should be counted. It also depends on if there's an objection raised by any of the parties about how to treat that ballot.

JUDGE: And what are some of the issues they're looking for on the ballot?

HAAS: It could be, for instance, whether or not the ballot was initialed by the clerk. There are some technical requirements that are required for the ballot to be counted. There could be objections raised as to whether or not that ballot should be tabulated.

JUDGE: Do they also look at the ballot and see if it's been filled out dark enough or anything of that nature?

HAAS: They could be inspecting for those reasons as well.

JUDGE: And finally, does the State or the Commission undertake any audits of its vendors to inspect their security, their computer security?

HAAS: We do not do visits of their locations. As I've said, there are a number of conditions that apply to each approval, but we don't audit their security procedures.

JUDGE: Any follow-up questions?

STATE ATTORNEY: You mentioned the Internet transmission of some results. Are those the final results?

HAAS: Those are the unofficial election results, not the official results.

JUDGE: You may step down. Thank you.

STEIN'S CLOSING

Good evening, Your Honor. Our client, Jill Stein, thanks you for entertaining this and recognizing how important it is. We're not surprised that it's being taken seriously, because ensuring that Wisconsin's votes are counted accurately, and in no way compromised by any claims of intentional misconduct or otherwise, is obviously profoundly important to the people of this state and frankly to all citizens of this country and our democracy.

There are a couple things that we know based on the evidence that's been presented and otherwise are really basically beyond dispute.

We know that there will be a recount. We know that it's going to start Thursday morning. We know that it has been paid for by people other than the people of the state of Wisconsin, that it will not cost the taxpayers any money in that sense.

The only question is how that recount will be conducted. The central question is obviously whether it will be conducted uniformly by hand or whether some jurisdictions will be allowed to re-feed the same ballot into the same machine and functionally get what one expert testified to as the same --seeking a second opinion but from the same machine, and therefore, the same doctor.

The reason that this case comes here today in an unprecedented way is because these circumstances are unprecedented. This is the first time in any American election where there are sustained attacks, cyber-attacks, from foreign IP addresses, confirmed by the federal government, that have been successful all, aimed at our election systems, all aimed at potentially influencing the outcome of the election for President of the United States.

That is unprecedented, and that is a primary reason, the motivating reason, that brings us here today.

We also know that leading up to the election, the DNC was successfully hacked. One of the campaign managers for the Clinton campaign was successfully hacked. Hacked communications were released in order to have an impact on the election.

Illinois elections officials were successfully hacked and 200,000 voter records were taken or removed or stolen.

Arizona election officials had a hack where there was an intrusion and records were removed.

We also know from federal authorities and public reports that there were over 20 other attempts on other state election officials, offices, computers, and the like.

We know all of that. That's a fact.

We know that someone was attempting to influence this election through cyber means.

We know that they succeeded in some places.

And we also know, thankfully, that in Wisconsin, unlike some other jurisdictions, we have an absolute, reliable, verifiable way of determining whether that happened. It's right there before us.

And we're going to be recounting. So we know all of that. We know that about the attacks, but we also know about the study, which Professor Stark testified to, in which Professor Mebane detected evidence that indicates anomalies consistent with someone attempting to manipulate the results of the election in Wisconsin. That evidence exists—an anomaly that's consistent with potential manipulation. I had not heard of this kind of statistic testing before. But basically what he looked at is we have thousands of random numbers that had been generated, the vote tallies, in all of the wards, in all of the state of Wisconsin. There's what he called the terminal digit. That's just the last number in the string of numbers. And any kind of randomness, a statistician will tell you that that number should appear equally over time if you have a large enough sample, which we certainly do. And because of that, the means should always be somewhere within a deviation of the mean, which is 4.5. And he basically analyzed those final digits and concluded that in the smaller wards, there were anomalies consistent with some kind of potential interference.

Can we say that absolutely there was interference? No. If we could, we'd have a different kind of case than one just attempting to verify and make sure that there wasn't. But there are anomalies that are consistent with some kind of intrusion, and they're both on the Trump side and the Clinton side, and that's basically because they're consistent with the concept of manipulating the numbers in some fashion through three different kinds of tests.

And if that were actually happening, if somebody was manipulating that piece, there's no reason to believe that they weren't manipulating other potential parts of this election. So that's what we know coming in. That is what is exceptional.

We also know, and no one can seriously dispute, that all of the election systems, certainly including Wisconsin's (although it's not the worst), are absolutely vulnerable and susceptible to hacking and intrusion. There's no question about that.

There are officials who are working very hard in good faith following statutes that are appropriate for preventing the kind of script-kiddie sort of hacks that Professor Rivest testified to.

But they are woefully, woefully inadequate to prevent any concentrated attempt by a sophisticated group of people.

We know that those people exist and were trying to influence this election.

And we also know all of the vulnerabilities. Mr. Haas has testified about the kinds of tests that they do and all the rest. And there's no doubt that I think those tests can find some errors, correct some errors. We all want accountability and verification to some point.

But at the end of the day, all of the experts testified the systems are vulnerable, and they were unanimous. These are world-renowned experts. Professor Rivest is the person who invented the technology that secures our communications on the Internet to the maximum degree possible, the secure communications that we pay for things on over the Internet. He thought it was important enough to testify today to make it clear to the Court, along with Professor Halderman, that these systems are absolutely vulnerable to anybody who's sufficiently sophisticated, can absolutely infect them and change the outcome of the election.

The other thing that Dr. Halderman testified to that any sophisticated attempt to manipulate a vote would have by logic and common sense focused on states where there was likely to be a close margin. Because you don't want to try to manipulate an election that will create a result that is so widely divergent from what people expect that it would arouse suspicion and cause things like a recount by hand that would identify and verify that something had gone wrong. So, we know that Wisconsin was certainly in the very small subset of states that would be a logical and likely target on top of everything else.

So, at the end of the day, we've heard testimony, very clear testimony, that that recount is going to require that each ballot be examined and that everybody will have the right, including the candidates, to examine the ballot and even tabulate it on their own.

What we want to have is absolute confidence in the result of this election in the state of Wisconsin. And we don't know whether we'll discover anything, but it won't take much to change the outcome of this election. You had Professor Stark testifying very clearly and plainly just to be clear about what the issue is. All we need is 11,000 votes to change from one column to the next column for the outcome of the election in the state of Wisconsin for the President to change. That is less than 4 tenths of one percentage point. It is nothing.

The outcome could be changed by errors that are not attributable to some kind of attack, but at the same time that we're counting --and there's a potential of serious a substantial potential that the outcome of the election could be changed.

If we hand count every vote, then we will walk away from the process and every citizen of the country that we live in will know that this count was the most verified, accurate, reliable count of anywhere in the United States. It will be the only one that we're aware of that will be counted completely by hand.

And every expert has made it crystal clear and plain that hand counting is the only reliable methodology. That's the reason that they insist upon in all systems that make any sense a verifiable, auditable paper trail. And we have it in Wisconsin.

And we need to use it and not just shove those ballots back into the same machines that may have created a problem in the first place.

And that is the end of my argument. I urge the Court to appreciate the power, obviously, that the Court has, which I know you know, but to make equitable accurate way to conduct a recount is through a hand count. The experts testified to that. It was a gold standard for accuracy. It's the best way to ascertain vote intent, and it's the way that the State itself does its audit when it's trying to figure out if its count was correct.

We think there's no question that a hand count can be completed statewide in a timely fashion. Madison's doing it. Minnesota did a statewide count in five days. There's going to be a lot of work that goes into it, but there's going to be a lot of work that goes into this either way.

And then last I would just say, since we didn't have a chance to address the State's brief, that I think that the position the State has laid out in terms of how it's interpreting the governing statute can't be the right one because under the position they have put forward there would never be a hand recount in the state.

There's no way that the test that they have set forth could possibly be met. It's also a test not consistent with the basic principles that underlay Wisconsin's open government laws. It's brought access to government affairs generally and specifically with respect to recounts. It's also not consistent with the State's stated policy of doing everything possible to ascertain voter intent.

And so we think that all of the factors here need to be taken into account including the nature of the recount, the most accurate method, and transparency. So for those reasons we think that a hand recount is appropriate.

STATE'S CLOSING

Your Honor, one thing that's important here is what this case is not about. This is not a case about whether the general system of counting ballots automatically is a valid one --is a valid way to run an election. I can't give you a cite, but I know just from general exposure that that was litigated hard decades ago when the first automatic counting and scanning machines came into effect. That is not what is at issue here.

And the statute that controls here presumes the validity of the general system of automatic counting votes. The decision here is --at issue here is the statutory directive to give local canvassers the discretion to decide the best way to recount votes. A court can override that statutorily mandated discretion only by clear and convincing evidence of two things:

1. An irregularity or mistake in the automatic counting that will produce that produced an incorrect result, and
2. Independently, that a recount by hand will result in a substantial probability that the result will change.

There's no evidence presented today or in the papers of either of those. Not one of the experts testified that they know the problem with the Wisconsin election tabulation system or equipment.

In fact, every one of them confirmed the opposite. Mr. Mebane, of course, is not here. What we heard from is Professor Stark, an expert who did not do the study, who couldn't even answer the Court's questions about the information --the data that went in the study. And Professor Mebane concludes that you can't say that it was the result of any problem.

All that we have here is 100 percent hypothetical speculation about what could possibly, imaginably happen. That is far, far short of any standard. It's not clear and convincing evidence.

And this decision is not a probability. This isn't a motion to dismiss type of situation or a motion to dismiss on the pleadings. This is clear and convincing evidence, and we are not in the ballpark of that. The separate independent, branch that must be met is that the mistake produces a substantial probability that the result will change. There's been no evidence about that whatsoever. And with not great surprise the petitioner, Jill Stein, has said publicly that she does not think there's a likelihood of that, and her campaign manager said that that is not why this lawsuit was filed. We're left with, frankly, your Honor, not a close case. The statute presumes the system that is in effect. It gives local canvassers the discretion for them to choose the best way how to conduct this recount absent clear and convincing evidence, and we have not --we are not --the petitioner's not anywhere near that standard.

JUDGE: I want to say to you all before I take a break to reach my decision, I'm very impressed with your abilities, your preparedness to a very quick situation, your professionalism. This has been an amazing display of excellent lawyering. However my decision comes out, I want to thank all of you for your time and effort tonight, and we'll go from there. So I will try to come back as quickly as I can. Thank you.

JUDGES' DECISION

JUDGE: As I indicated before we started, I had read everything. I read all the affidavits, all the supporting detail, the briefs, and I appreciate the arguments of counsel and the witnesses.

What I want to say first is the people of Wisconsin have an absolute right to rely on the integrity of the voting process. The right to vote is the cornerstone of our democracy.

A recount isn't a threat. Instead, it should be an affirmation of the democratic process. And I think we can all agree that a hand recount is the gold standard. It's the best we can do, and I don't think there's any dispute to that.

We also can probably agree that there is no cost difference between a hand recount and recount as proposed by the various canvassing or the various counties, because of the fact that the petitioner is going to pay for it.

I also recognize that Dane County has affirmatively agreed to hand count the ballots. It is the second largest county in the state. And that is best way to determine the recount.

However, having said that, that's not the court's decision to decide what's the best way. That's not what I can do. I follow the law. That's who I am despite my personal opinions or what I feel is the best count. I have to do what the law tells me to do. And here the law is contained in 5.90(2), and it's a two-prong test.

The petitioner bears the burden of establishing by clear and convincing evidence that due to a irregularity, defect, or mistake committed during the voting process, the results of a recount using an automatic tabulating equipment will produce an incorrect recount result, and—this is second prong—that there is a substantial probability that recounting the ballots by hand, or another method, will produce a more correct result and change the outcome of the election.

Based on the evidence, even if I find that there is a substantial probability that recounting the ballots by hand will produce a more correct result, which I think is undisputed, and even if I find that change the outcome of the election is met here because the outcome of the election is ambiguous doesn't mean it switches from what was originally a victory for Trump is now a victory for Clinton even if that is sufficient or it's just the number of votes change.

So, even if I find the second prong has been met here, I still have a problem with the first prong. It's clear and convincing evidence that due to a defect or mistake or something else committed during the voting that the results of recount using the equipment will produce an incorrect recount result.

So, what is clear and convincing? The burden of proof, at least in Wisconsin jury instructions, indicate that clear, satisfactory, and convincing evidence is evidence which when weighed against that opposed it clearly has more convincing power. It is evidence which satisfies and convinces you that 'yes' should be the answer because of its greater weight and clear, convincing power.

So, the testimony today has been that the experts have said there is a chance that the machines could have been hacked or that there are other problems with the machines, that they don't read correctly, all of which may be true, but there's nothing to link it to Wisconsin. There has to be a link to something during the voting process. There hasn't been that link established here.

There has been the small --there has been the allegation about the small wards that one of the other professors, his study, but he hasn't been here today. His own study indicated that he can't tell you why the outcome. And it is something that an expert can rely on under s.907.03, Wis. Stats, but it is inadmissible hearsay evidence. Though the testifying professor can rely on it in his opinions, and I did take his opinions into weight.

But all of the experts indicated that yes, there are these potential issues. And I understand the problem. The problem is you don't know there's going to be an issue until you do it.

But under the statute, I can't speculate. I have to find by clear and convincing evidence that there is some sort of defect, mistake, or irregularity committed during the voting process that would cause the recount using the automatic tabulating equipment to have incorrect recount results. And I don't find by clear and convincing evidence that occurred here.

So then we default back to s.5.90(1), which allows the board canvassers to determine how they're going to do the recount --and the fact that they want to do a recount using the machines is their decision, it's their discretion.

I may disagree with it. I may see that the hand ballots is the best way. I think we would all agree with that.

But I can't put myself in their position. I understand it is extremely important to the people of the state of Wisconsin. I understand that it is extremely important to the nation. But I must follow the law, and the law as set forth in 5.90(2) is there for a reason. And I just do not find clear and convincing evidence. So, that is my decision.

I'm going to allow the 19 counties to do the recount the way that they intended. Again, I think everybody would strongly encourage them to do the hand recount, but it is their decision, and that is the legislative function is to make the statutes, and in this situation, I don't have any authority to decide what is the best for those counties. So, that's my decision.